SECS1028 - Laboratoire 8 - centralisation des logs (suite)

laboratoire not´e (test de mi-session) sur 23 points - 20% de la note finale

a` rendre pour le 17 mars

Objectif du laboratoire : centraliser les logs sur un serveur d´edi´e

Pour ce laboratoire, utilisez une VM Kali Purple (VM de controle), une VM DVWA, une VM FreeBSD et une VM Linux (serveur des logs) sur le r´eseau interne de VirtualBox.

Notez ci-dessous les adresses IP de ces VM sur le r´eseau interne VirtualBox:

Kali Purple : 192.168.2.8

DVWA : 192.168.2.7

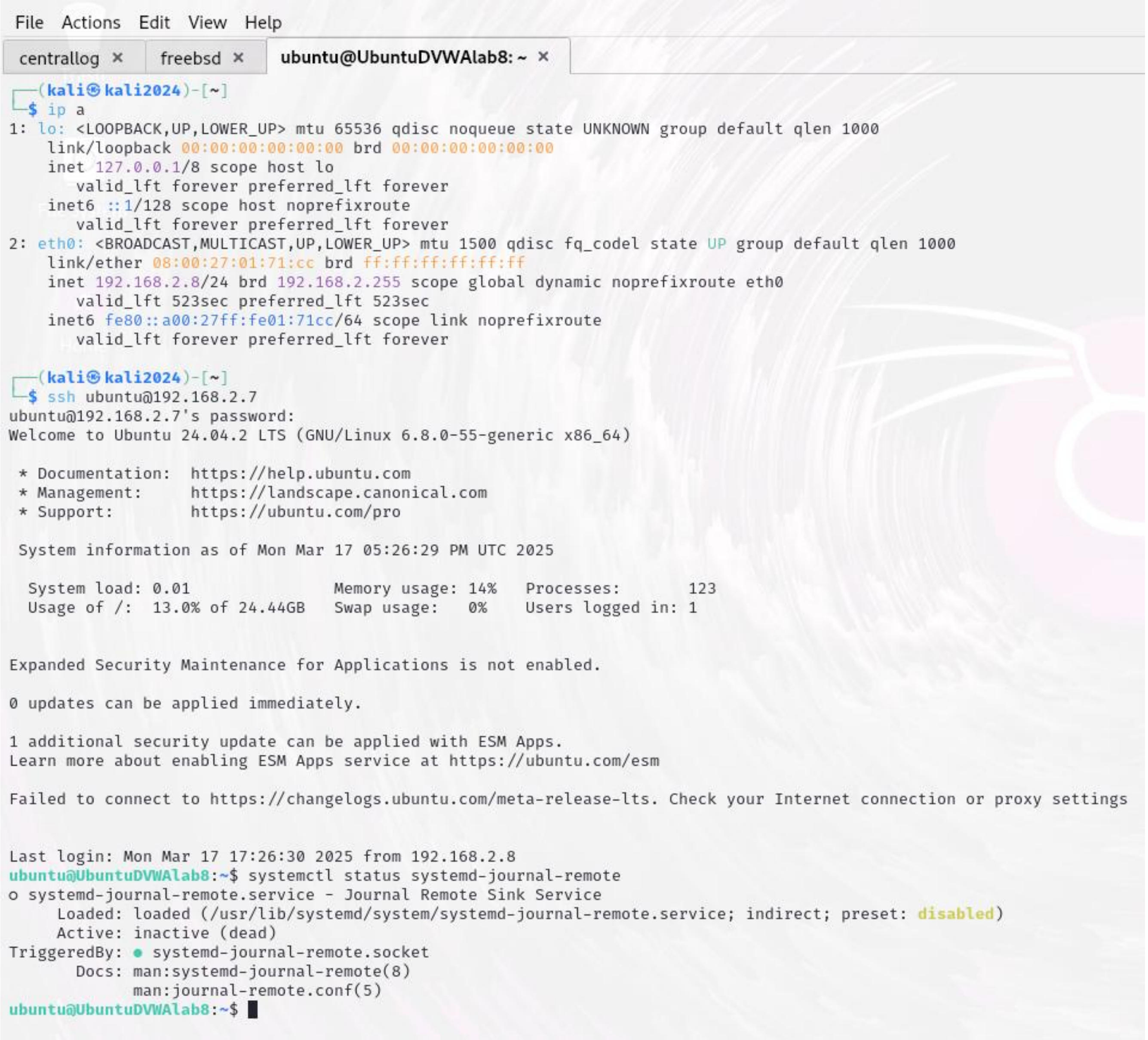
Linux (log centralisé): 192.168.2.5

Freebsd :192.168.2.9

1 DVWA (5 points)

L'objectif de cette partie est de centraliser les logs produits par la VM DVWA vers le serveur de Logs.

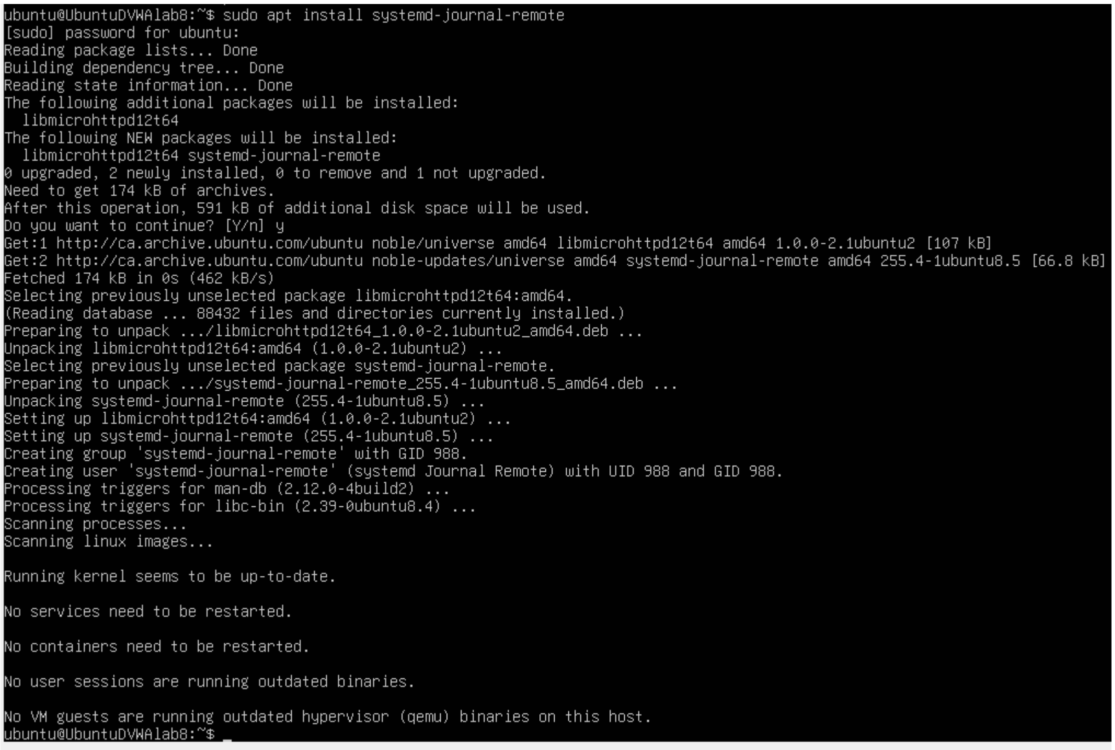
1) Installez sur VirtualBox une VM Linux qui sera le serveur des logs centralis´es. (1 point)



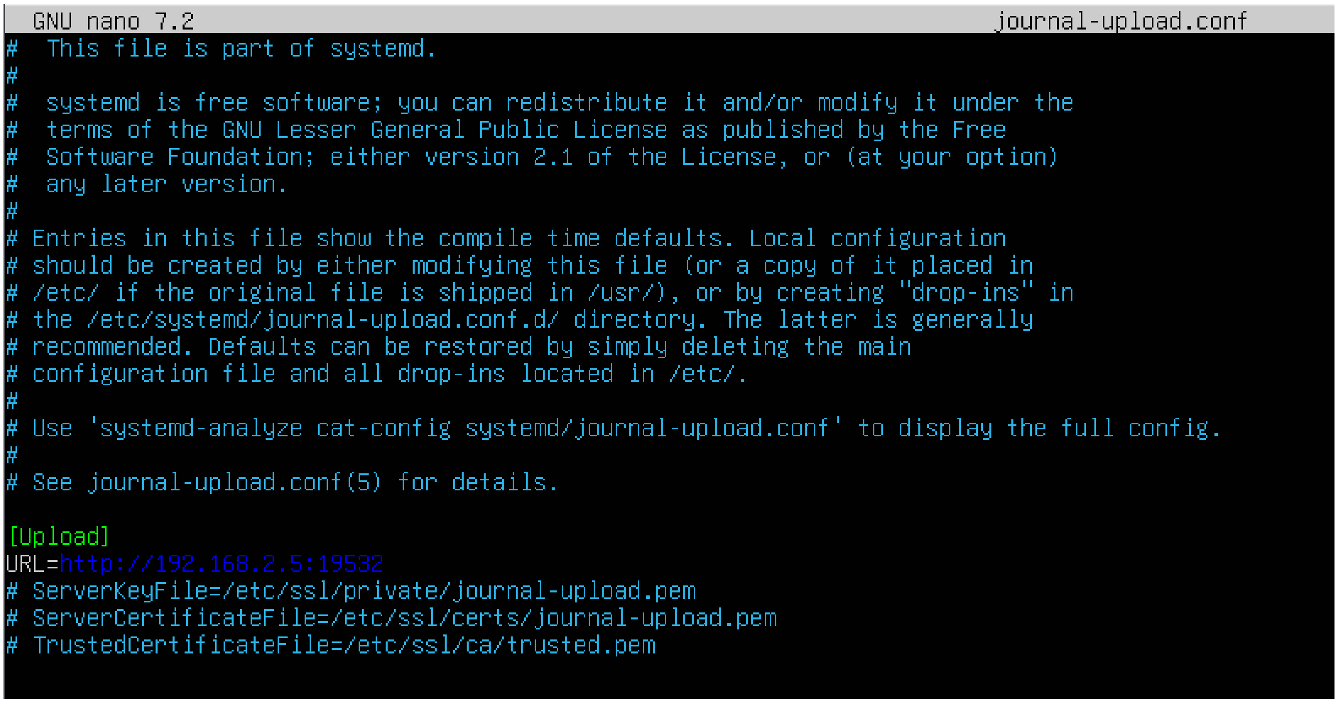
```
┌──(kali㉿kali2024)-[~]
└─$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:01:71:cc brd ff:ff:ff:ff:ff:ff
    inet 192.168.2.8/24 brd 192.168.2.255 scope global dynamic noprefixroute eth0
       valid_lft 523sec preferred_lft 523sec
    inet6 fe80::a00:27ff:fe01:71cc/64 scope link noprefixroute
       valid_lft forever preferred_lft forever

┌──(kali㉿kali2024)-[~]
└─$ ssh ubuntu@192.168.2.7
ubuntu@192.168.2.7's password:
Welcome to Ubuntu 24.04.2 LTS (GNU/Linux 6.8.0-55-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/pro

 System information as of Mon Mar 17 05:26:29 PM UTC 2025

  System load: 0.01              Memory usage: 14%   Processes:       123
  Usage of /:  13.0% of 24.44GB   Swap usage:   0%    Users logged in: 1


Expanded Security Maintenance for Applications is not enabled.

0 updates can be applied immediately.

1 additional security update can be applied with ESM Apps.
Learn more about enabling ESM Apps service at https://ubuntu.com/esm

Failed to connect to https://changelogs.ubuntu.com/meta-release-lts. Check your Internet connection or proxy settings


Last login: Mon Mar 17 17:26:30 2025 from 192.168.2.8
ubuntu@UbuntuDVWAlab8:~$ systemctl status systemd-journal-remote
○ systemd-journal-remote.service - Journal Remote Sink Service
     Loaded: loaded (/usr/lib/systemd/system/systemd-journal-remote.service; indirect; preset: disabled)
     Active: inactive (dead)
TriggeredBy: ● systemd-journal-remote.socket
       Docs: man:systemd-journal-remote(8)
             man:journal-remote.conf(5)
ubuntu@UbuntuDVWAlab8:~$ █
```

2) Proposez une solution pour transf´erer les logs de DVWA vers le serveur de logs. D´ecrivez la solution que vous avez choisie a` l'aide d'explications textuelles et de captures ´ecran de sa mise en place. (2 points)

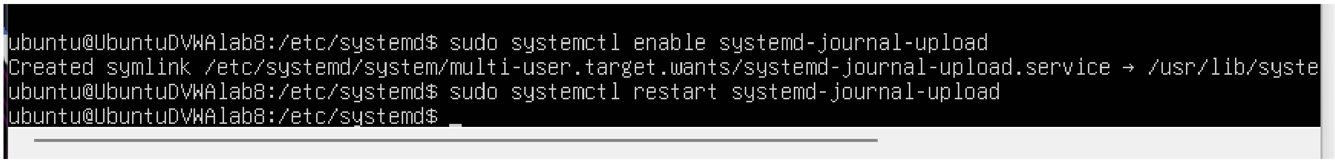
Systemd-journal-remote sur log centraliser et DVWA



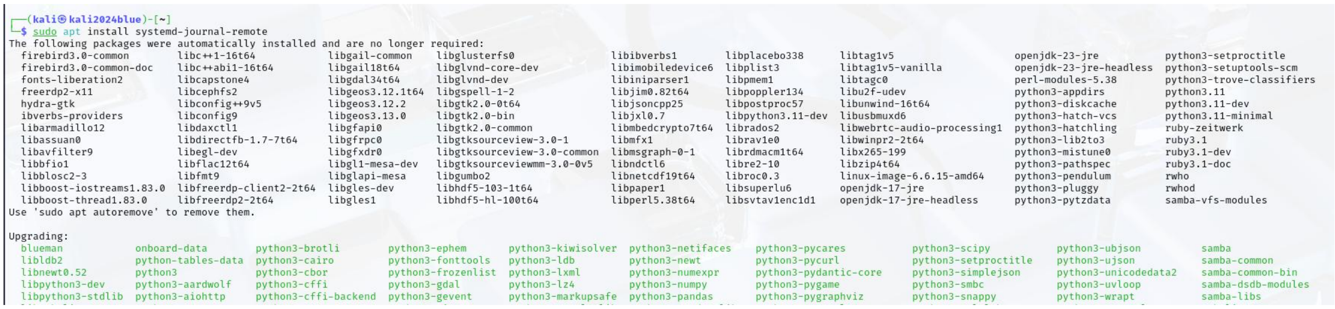
```
ubuntu@UbuntuDVWAlab8:~$ sudo apt install systemd-journal-remote
[sudo] password for ubuntu:
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  libmicrohttpd12t64
The following NEW packages will be installed:
  libmicrohttpd12t64 systemd-journal-remote
0 upgraded, 2 newly installed, 0 to remove and 1 not upgraded.
Need to get 174 kB of archives.
After this operation, 591 kB of additional disk space will be used.
Do you want to continue? [Y/n] y
Get:1 http://ca.archive.ubuntu.com/ubuntu noble/universe amd64 libmicrohttpd12t64 amd64 1.0.0-2.1ubuntu2 [107 kB]
Get:2 http://ca.archive.ubuntu.com/ubuntu noble-updates/universe amd64 systemd-journal-remote amd64 255.4-1ubuntu8.5 [66.8 kB]
Fetched 174 kB in 0s (462 kB/s)
Selecting previously unselected package libmicrohttpd12t64:amd64.
(Reading database ... 88432 files and directories currently installed.)
Preparing to unpack .../libmicrohttpd12t64_1.0.0-2.1ubuntu2_amd64.deb ...
Unpacking libmicrohttpd12t64:amd64 (1.0.0-2.1ubuntu2) ...
Selecting previously unselected package systemd-journal-remote.
Preparing to unpack .../systemd-journal-remote_255.4-1ubuntu8.5_amd64.deb ...
Unpacking systemd-journal-remote (255.4-1ubuntu8.5) ...
Setting up libmicrohttpd12t64:amd64 (1.0.0-2.1ubuntu2) ...
Setting up systemd-journal-remote (255.4-1ubuntu8.5) ...
Creating group 'systemd-journal-remote' with GID 988.
Creating user 'systemd-journal-remote' (systemd Journal Remote) with UID 988 and GID 988.
Processing triggers for man-db (2.12.0-4build2) ...
Processing triggers for libc-bin (2.39-0ubuntu8.4) ...
Scanning processes...
Scanning linux images...

Running kernel seems to be up-to-date.

No services need to be restarted.

No containers need to be restarted.

No user sessions are running outdated binaries.

No VM guests are running outdated hypervisor (qemu) binaries on this host.
ubuntu@UbuntuDVWAlab8:~$ _
```



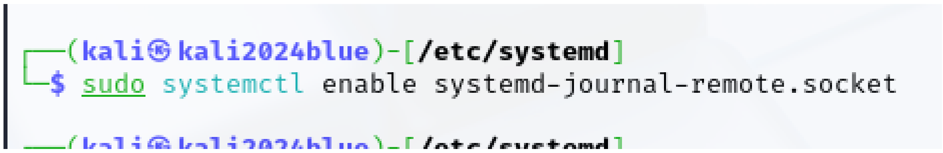
```
  GNU nano 7.2                                                      journal-upload.conf
#  This file is part of systemd.
#
#  systemd is free software; you can redistribute it and/or modify it under the
#  terms of the GNU Lesser General Public License as published by the Free
#  Software Foundation; either version 2.1 of the License, or (at your option)
#  any later version.
#
# Entries in this file show the compile time defaults. Local configuration
# should be created by either modifying this file (or a copy of it placed in
# /etc/ if the original file is shipped in /usr/), or by creating "drop-ins" in
# the /etc/systemd/journal-upload.conf.d/ directory. The latter is generally
# recommended. Defaults can be restored by simply deleting the main
# configuration file and all drop-ins located in /etc/.
#
# Use 'systemd-analyze cat-config systemd/journal-upload.conf' to display the full config.
#
# See journal-upload.conf(5) for details.

[Upload]
URL=http://192.168.2.5:19532
# ServerKeyFile=/etc/ssl/private/journal-upload.pem
# ServerCertificateFile=/etc/ssl/certs/journal-upload.pem
# TrustedCertificateFile=/etc/ssl/ca/trusted.pem
```



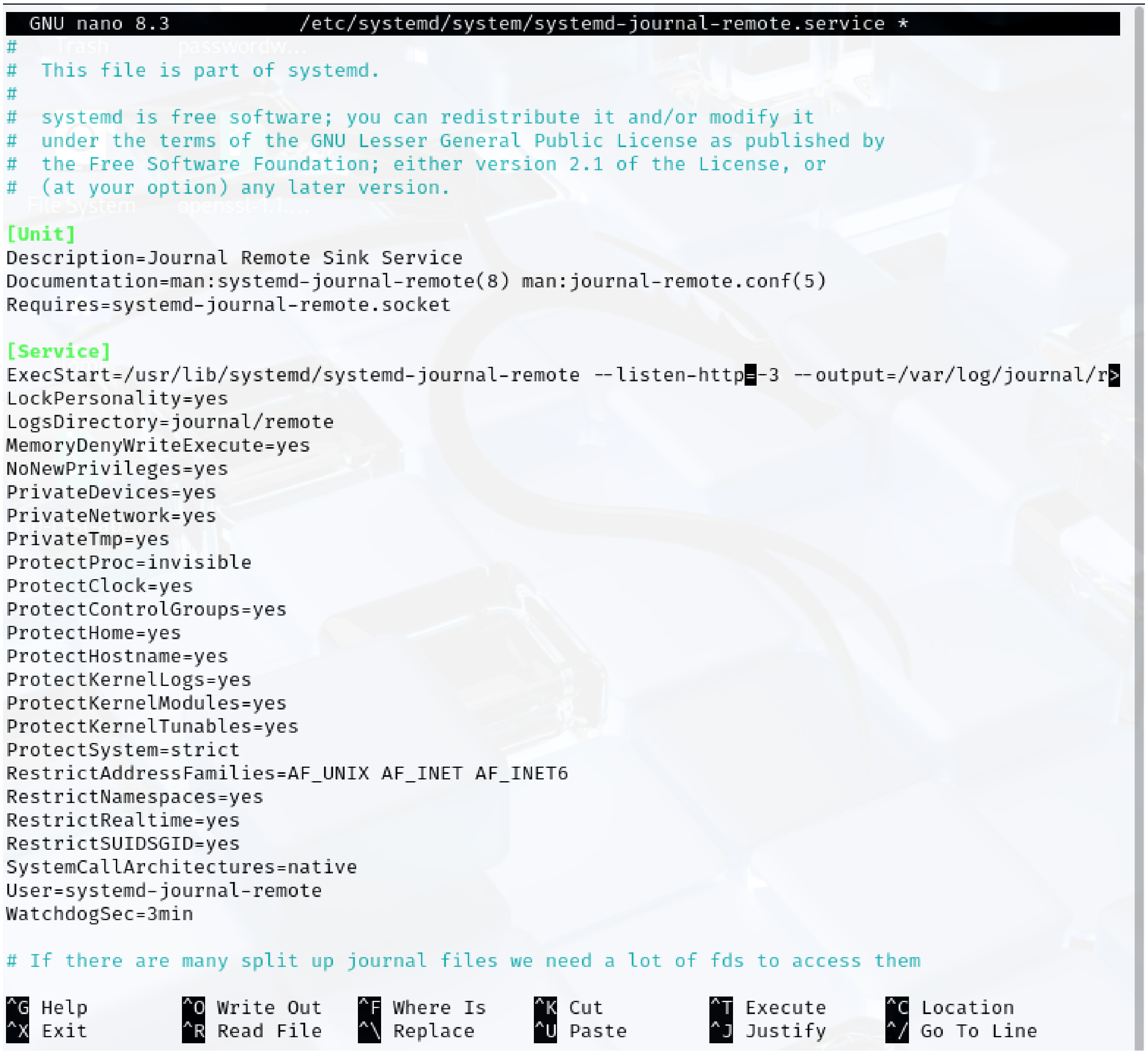
```
ubuntu@UbuntuDVWAlab8:/etc/systemd$ sudo systemctl enable systemd-journal-upload
Created symlink /etc/systemd/system/multi-user.target.wants/systemd-journal-upload.service → /usr/lib/syste
ubuntu@UbuntuDVWAlab8:/etc/systemd$ sudo systemctl restart systemd-journal-upload
ubuntu@UbuntuDVWAlab8:/etc/systemd$ _
```



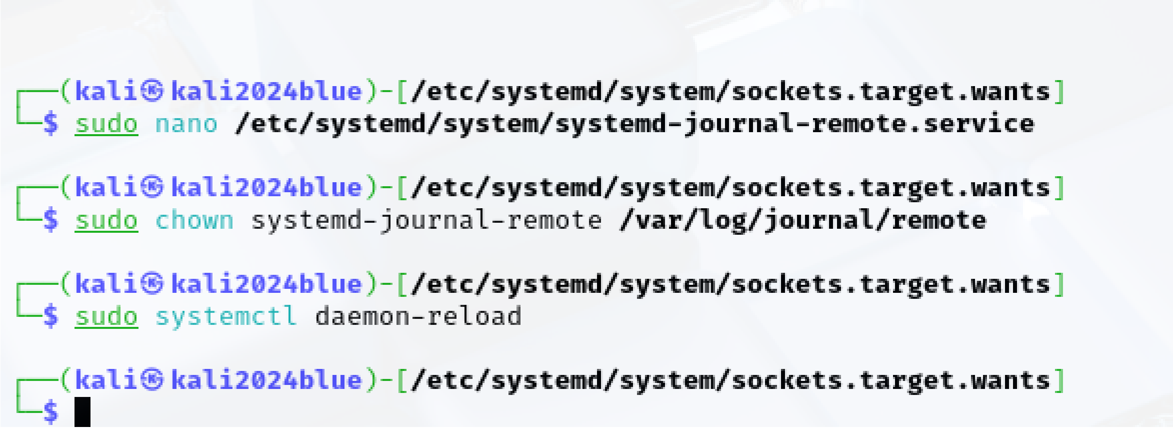
```
┌──(kali㉿kali2024blue)-[~]
└─$ sudo apt install systemd-journal-remote
The following packages were automatically installed and are no longer required:
  firebird3.0-common        libc++1-16t64              libgail-common    libglusterfs0                   libibverbs1        libplacebo338       libtag1v5                       openjdk-23-jre            python3-setproctitle
  firebird3.0-common-doc    libc++abi1-16t64           libgail18t64      libglvnd-core-dev               libimobiledevice6  libplist3           libtag1v5-vanilla               openjdk-23-jre-headless   python3-setuptools-scm
  fonts-liberation2         libcapstone4               libgdal34t64      libglvnd-dev                    libiniparser1      libpmem1            libtagc0                        perl-modules-5.38         python3-trove-classifiers
  freerdp2-x11              libcephfs2                 libgeos3.12.1t64  libgspell-1-2                   libjim0.82t64      libpoppler134       libu2f-udev                     python3-appdirs           python3.11
  hydra-gtk                 libconfig++9v5             libgeos3.12.2     libgtk2.0-0t64                  libjsoncpp25       libpostproc57       libunwind-16t64                 python3-diskcache         python3.11-dev
  ibverbs-providers         libconfig9                 libgeos3.13.0     libgtk2.0-bin                   libjxl0.7          libpython3.11-dev   libusbmuxd6                     python3-hatch-vcs         python3.11-minimal
  libarmadillo12            libdaxctl1                 libgfapi0         libgtk2.0-common                libmbedcrypto7t64  librados2           libwebrtc-audio-processing1     python3-hatchling         ruby-zeitwerk
  libassuan0                libdirectfb-1.7-7t64       libgfrpc0         libgtksourceview-3.0-1          libmfx1            librav1e0           libwinpr2-2t64                  python3-lib2to3           ruby3.1
  libavfilter9              libegl-dev                 libgfxdr0         libgtksourceview-3.0-common     libmsgraph-0-1     librdmacm1t64       libx265-199                     python3-mistune0          ruby3.1-dev
  libbfio1                  libflac12t64               libgl1-mesa-dev   libgtksourceviewmm-3.0-0v5      libndctl6          libre2-10           libzip4t64                      python3-pathspec          ruby3.1-doc
  libblosc2-3               libfmt9                    libglapi-mesa     libgumbo2                       libnetcdf19t64     libroc0.3           linux-image-6.6.15-amd64        python3-pendulum          rwho
  libboost-iostreams1.83.0  libfreerdp-client2-2t64    libgles-dev       libhdf5-103-1t64                libpaper1          libsuperlu6         openjdk-17-jre                  python3-pluggy            rwhod
  libboost-thread1.83.0     libfreerdp2-2t64           libgles1          libhdf5-hl-100t64               libperl5.38t64     libsvtav1enc1d1     openjdk-17-jre-headless         python3-pytzdata          samba-vfs-modules
Use 'sudo apt autoremove' to remove them.

Upgrading:
  blueman            onboard-data        python3-brotli        python3-ephem        python3-kiwisolver  python3-netifaces  python3-pycares          python3-scipy         python3-ubjson         samba
  libldb2            python-tables-data  python3-cairo         python3-fonttools    python3-ldb         python3-newt       python3-pycurl           python3-setproctitle  python3-ujson          samba-common
  libnewt0.52        python3             python3-cbor          python3-frozenlist   python3-lxml        python3-numexpr    python3-pydantic-core    python3-simplejson    python3-unicodedata2   samba-common-bin
  libpython3-dev     python3-aardwolf    python3-cffi          python3-gdal         python3-lz4         python3-numpy      python3-pygame           python3-smbc          python3-uvloop         samba-dsdb-modules
  libpython3-stdlib  python3-aiohttp     python3-cffi-backend  python3-gevent       python3-markupsafe  python3-pandas     python3-pygraphviz       python3-snappy        python3-wrapt          samba-libs
```



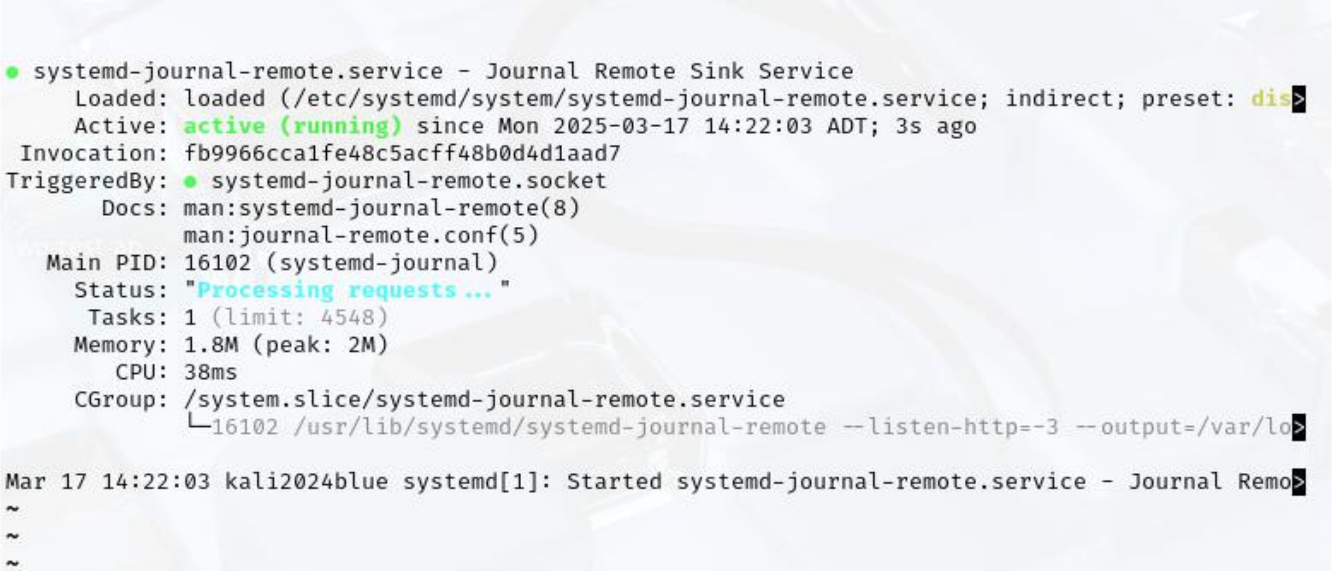
```
┌──(kali㉿kali2024blue)-[/etc/systemd]
└─$ sudo systemctl enable systemd-journal-remote.socket

┌──(kali㉿kali2024blue)-[/etc/systemd]
```



```
  GNU nano 8.3              /etc/systemd/system/systemd-journal-remote.service *
#
#  This file is part of systemd.
#
#  systemd is free software; you can redistribute it and/or modify it
#  under the terms of the GNU Lesser General Public License as published by
#  the Free Software Foundation; either version 2.1 of the License, or
#  (at your option) any later version.

[Unit]
Description=Journal Remote Sink Service
Documentation=man:systemd-journal-remote(8) man:journal-remote.conf(5)
Requires=systemd-journal-remote.socket

[Service]
ExecStart=/usr/lib/systemd/systemd-journal-remote --listen-http=-3 --output=/var/log/journal/r>
LockPersonality=yes
LogsDirectory=journal/remote
MemoryDenyWriteExecute=yes
NoNewPrivileges=yes
PrivateDevices=yes
PrivateNetwork=yes
PrivateTmp=yes
ProtectProc=invisible
ProtectClock=yes
ProtectControlGroups=yes
ProtectHome=yes
ProtectHostname=yes
ProtectKernelLogs=yes
ProtectKernelModules=yes
ProtectKernelTunables=yes
ProtectSystem=strict
RestrictAddressFamilies=AF_UNIX AF_INET AF_INET6
RestrictNamespaces=yes
RestrictRealtime=yes
RestrictSUIDSGID=yes
SystemCallArchitectures=native
User=systemd-journal-remote
WatchdogSec=3min

# If there are many split up journal files we need a lot of fds to access them

^G Help        ^O Write Out   ^F Where Is    ^K Cut         ^T Execute     ^C Location
^X Exit        ^R Read File   ^\ Replace     ^U Paste       ^J Justify     ^/ Go To Line
```

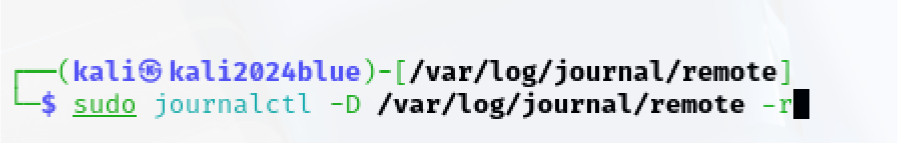


```
┌──(kali㉿kali2024blue)-[/etc/systemd/system/sockets.target.wants]
└─$ sudo nano /etc/systemd/system/systemd-journal-remote.service

┌──(kali㉿kali2024blue)-[/etc/systemd/system/sockets.target.wants]
└─$ sudo chown systemd-journal-remote /var/log/journal/remote

┌──(kali㉿kali2024blue)-[/etc/systemd/system/sockets.target.wants]
└─$ sudo systemctl daemon-reload

┌──(kali㉿kali2024blue)-[/etc/systemd/system/sockets.target.wants]
└─$ 
```

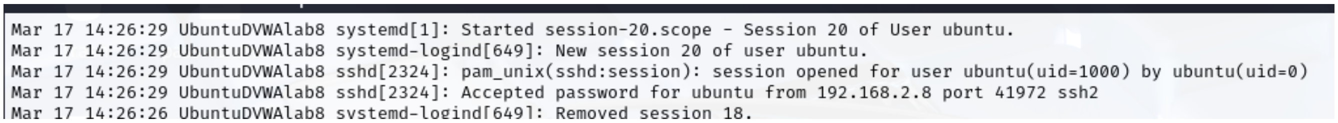


```
● systemd-journal-remote.service - Journal Remote Sink Service
     Loaded: loaded (/etc/systemd/system/systemd-journal-remote.service; indirect; preset: dis>
     Active: active (running) since Mon 2025-03-17 14:22:03 ADT; 3s ago
 Invocation: fb9966cca1fe48c5acff48b0d4d1aad7
TriggeredBy: ● systemd-journal-remote.socket
       Docs: man:systemd-journal-remote(8)
             man:journal-remote.conf(5)
   Main PID: 16102 (systemd-journal)
     Status: "Processing requests ..."
      Tasks: 1 (limit: 4548)
     Memory: 1.8M (peak: 2M)
        CPU: 38ms
     CGroup: /system.slice/systemd-journal-remote.service
             └─16102 /usr/lib/systemd/systemd-journal-remote --listen-http=-3 --output=/var/lo>

Mar 17 14:22:03 kali2024blue systemd[1]: Started systemd-journal-remote.service - Journal Remo>
~
~
~
```

3) D´emontrez que la solution fonctionne en vous connectant en ssh sur DVWA et en montrant les logs correpondant sur le serveur de logs (captures ´ecran). (2 points)



```
┌──(kali㉿kali2024blue)-[/var/log/journal/remote]
└─$ sudo journalctl -D /var/log/journal/remote -r
```

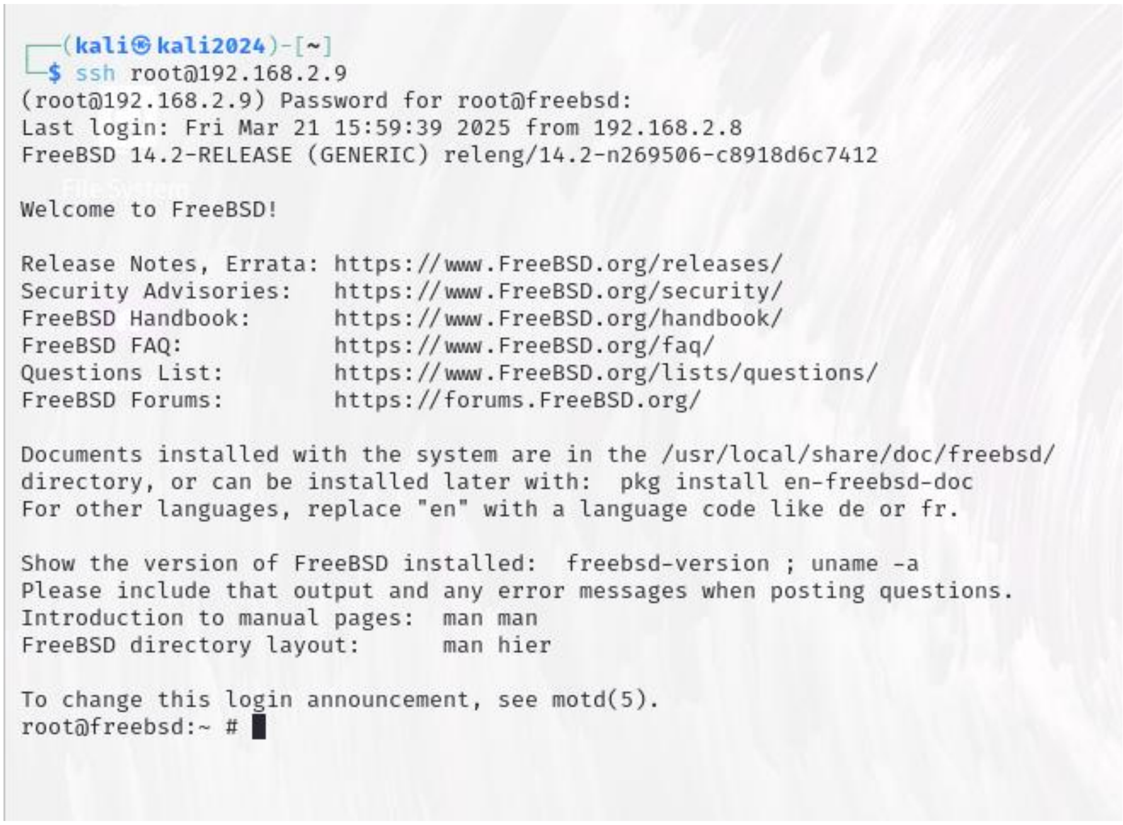


```
Mar 17 14:26:29 UbuntuDVWAlab8 systemd[1]: Started session-20.scope - Session 20 of User ubuntu.
Mar 17 14:26:29 UbuntuDVWAlab8 systemd-logind[649]: New session 20 of user ubuntu.
Mar 17 14:26:29 UbuntuDVWAlab8 sshd[2324]: pam_unix(sshd:session): session opened for user ubuntu(uid=1000) by ubuntu(uid=0)
Mar 17 14:26:29 UbuntuDVWAlab8 sshd[2324]: Accepted password for ubuntu from 192.168.2.8 port 41972 ssh2
Mar 17 14:26:26 UbuntuDVWAlab8 systemd-logind[649]: Removed session 18.
```

2 FreeBSD (6 points)

L’objectif de cette partie est de centraliser les logs produits par une VM FreeBSD (et qui utilise un service diff´erent de DVWA) vers le serveur de logs.

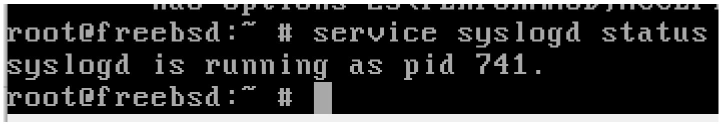
1) Installez sous VirtualBox une VM FreeBSD avec un serveur ssh activ´e. Faites une capture ´ecran de cette VM et une autre de la connexion ssh sur cette VM a` partir de Kali purple. (1 point)



```
┌──(kali㉿kali2024)-[~]
└─$ ssh root@192.168.2.9
(root@192.168.2.9) Password for root@freebsd:
Last login: Fri Mar 21 15:59:39 2025 from 192.168.2.8
FreeBSD 14.2-RELEASE (GENERIC) releng/14.2-n269506-c8918d6c7412

Welcome to FreeBSD!

Release Notes, Errata: https://www.FreeBSD.org/releases/
Security Advisories:   https://www.FreeBSD.org/security/
FreeBSD Handbook:      https://www.FreeBSD.org/handbook/
FreeBSD FAQ:           https://www.FreeBSD.org/faq/
Questions List:        https://www.FreeBSD.org/lists/questions/
FreeBSD Forums:        https://forums.FreeBSD.org/

Documents installed with the system are in the /usr/local/share/doc/freebsd/
directory, or can be installed later with:  pkg install en-freebsd-doc
For other languages, replace "en" with a language code like de or fr.

Show the version of FreeBSD installed:  freebsd-version ; uname -a
Please include that output and any error messages when posting questions.
Introduction to manual pages:  man man
FreeBSD directory layout:      man hier

To change this login announcement, see motd(5).
root@freebsd:~ #
```

2) Par d´efaut, quel service de logs est install´e sur FreeBSD ? Montrez une capture ´ecran du statut du service. (1 point).

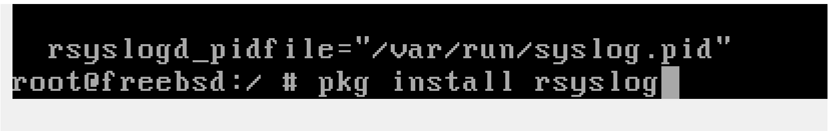
Syslog



```
root@freebsd:~ # service syslogd status
syslogd is running as pid 741.
root@freebsd:~ #
```

3) Proposez une solution permettant de transf´erer les logs de cette VM vers le serveur de logs. D´ecrivez cette solution a` l'aide d'explications textuelles et de captures ´ecran de sa mise en place. (2 points)

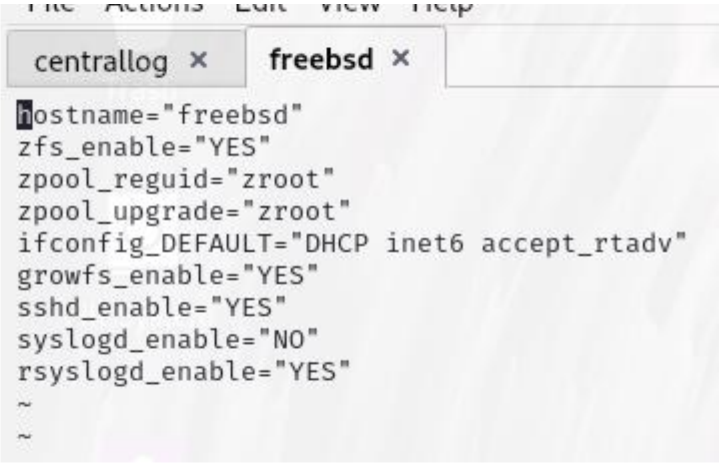
Installation de rsyslog sur les Freebsd



```
  rsyslogd_pidfile="/var/run/syslog.pid"
root@freebsd:/ # pkg install rsyslog
```

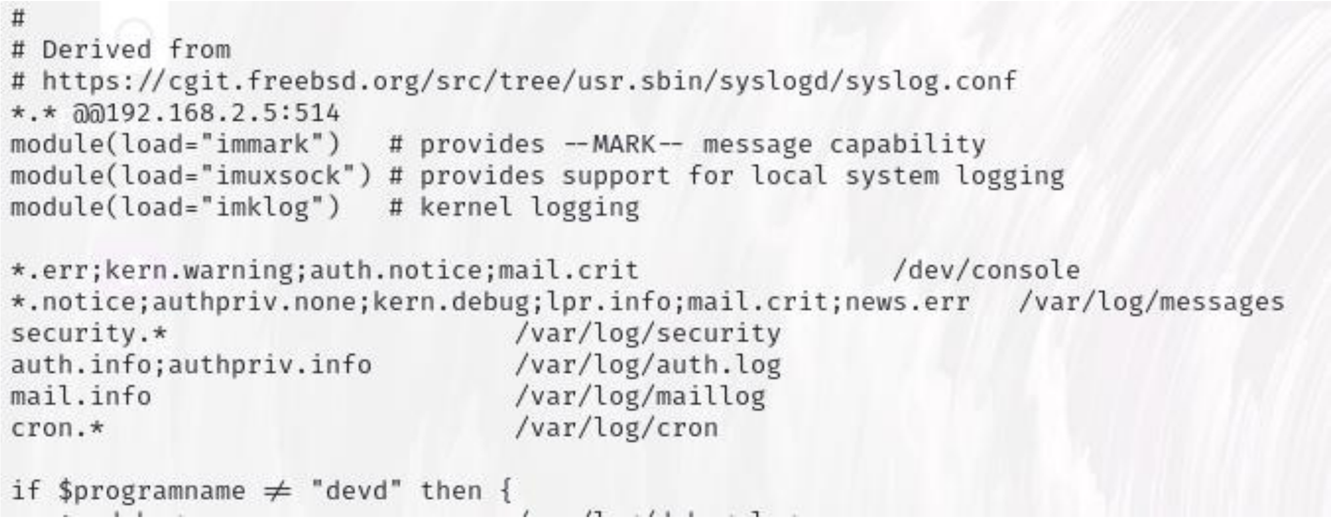
Configuration sur Freebsd

Dans le fichier rc.d

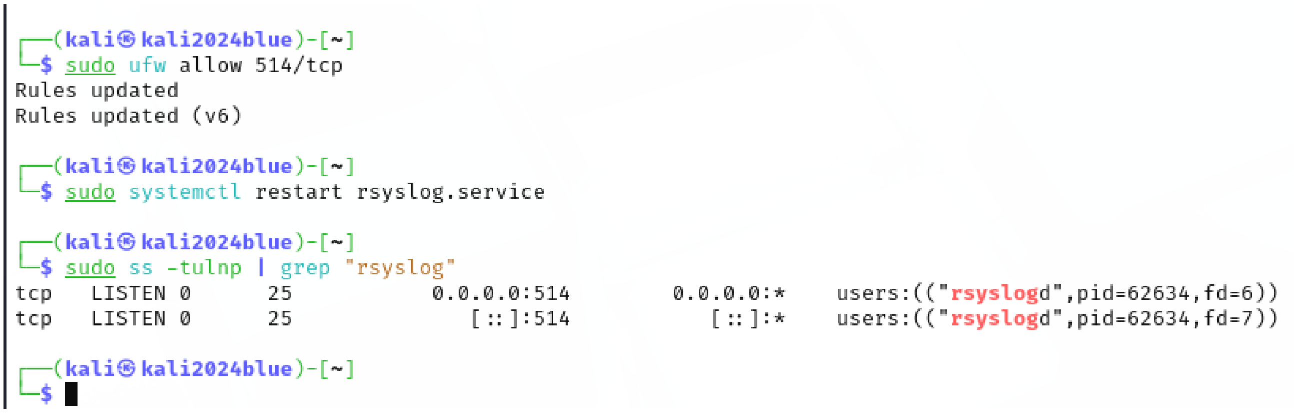


```
hostname="freebsd"
zfs_enable="YES"
zpool_reguid="zroot"
zpool_upgrade="zroot"
ifconfig_DEFAULT="DHCP inet6 accept_rtadv"
growfs_enable="YES"
sshd_enable="YES"
syslogd_enable="NO"
rsyslogd_enable="YES"
~
~
```

Dans le fichier le fichier /usr/local/etc/rsyslog.conf sur la freebsd

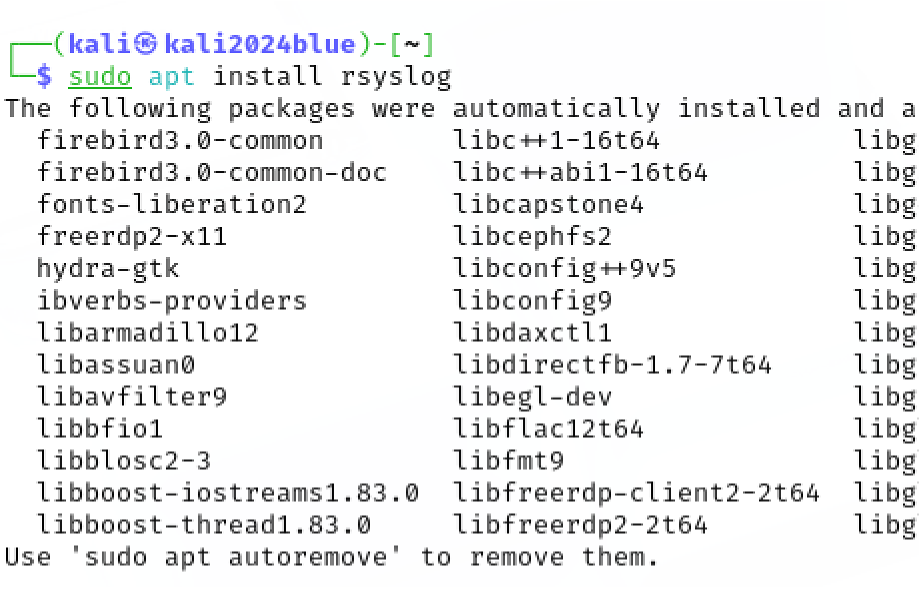


```
#
# Derived from
# https://cgit.freebsd.org/src/tree/usr.sbin/syslogd/syslog.conf
*.* @@192.168.2.5:514
module(load="immark")   # provides --MARK-- message capability
module(load="imuxsock") # provides support for local system logging
module(load="imklog")   # kernel logging

*.err;kern.warning;auth.notice;mail.crit                /dev/console
*.notice;authpriv.none;kern.debug;lpr.info;mail.crit;news.err   /var/log/messages
security.*                      /var/log/security
auth.info;authpriv.info         /var/log/auth.log
mail.info                       /var/log/maillog
cron.*                          /var/log/cron

if $programname ≠ "devd" then {
```



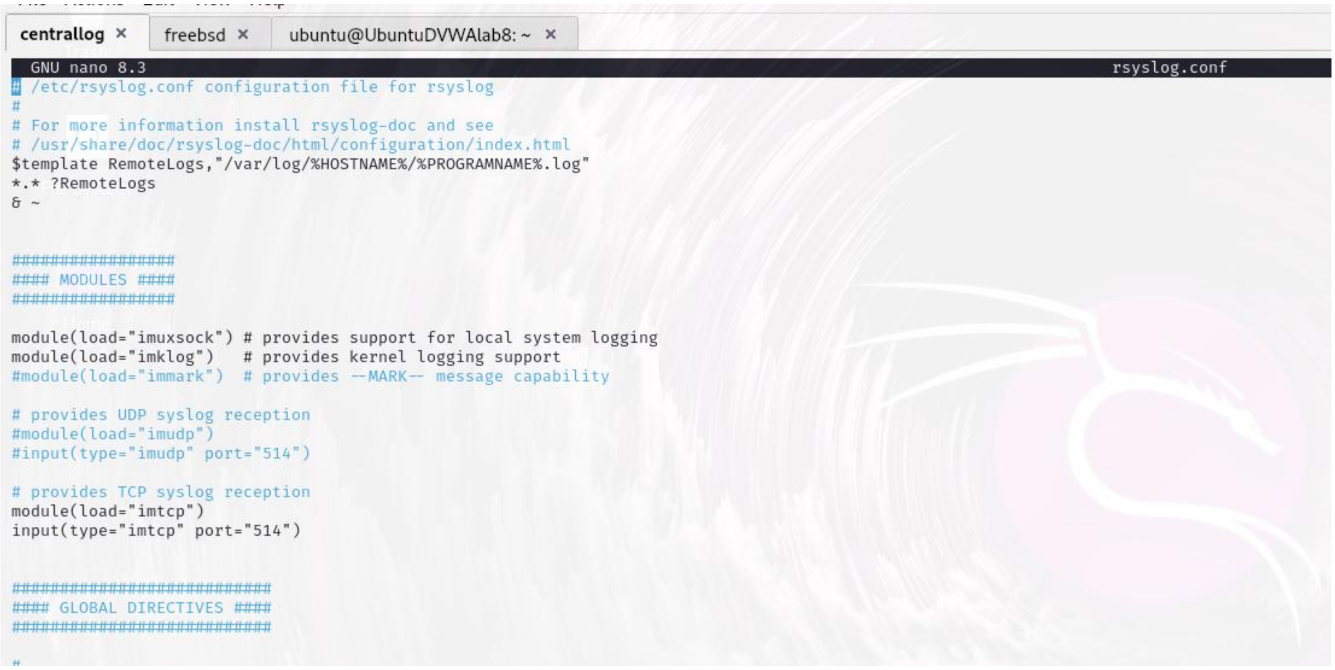
```
┌──(kali㉿kali2024blue)-[~]
└─$ sudo ufw allow 514/tcp
Rules updated
Rules updated (v6)

┌──(kali㉿kali2024blue)-[~]
└─$ sudo systemctl restart rsyslog.service

┌──(kali㉿kali2024blue)-[~]
└─$ sudo ss -tulnp | grep "rsyslog"
tcp    LISTEN 0      25          0.0.0.0:514        0.0.0.0:*     users:(("rsyslogd",pid=62634,fd=6))
tcp    LISTEN 0      25             [::]:514           [::]:*     users:(("rsyslogd",pid=62634,fd=7))

┌──(kali㉿kali2024blue)-[~]
└─$ 
```

Installation et configuration sur le serveur de log



```
┌──(kali㉿kali2024blue)-[~]
└─$ sudo apt install rsyslog
The following packages were automatically installed and a
  firebird3.0-common         libc++1-16t64           libg
  firebird3.0-common-doc     libc++abi1-16t64        libg
  fonts-liberation2          libcapstone4            libg
  freerdp2-x11               libcephfs2              libg
  hydra-gtk                  libconfig++9v5          libg
  ibverbs-providers          libconfig9              libg
  libarmadillo12             libdaxctl1              libg
  libassuan0                 libdirectfb-1.7-7t64    libg
  libavfilter9               libegl-dev              libg
  libbfio1                   libflac12t64            libg
  libblosc2-3                libfmt9                 libg
  libboost-iostreams1.83.0   libfreerdp-client2-2t64 libg
  libboost-thread1.83.0      libfreerdp2-2t64        libg
Use 'sudo apt autoremove' to remove them.
```

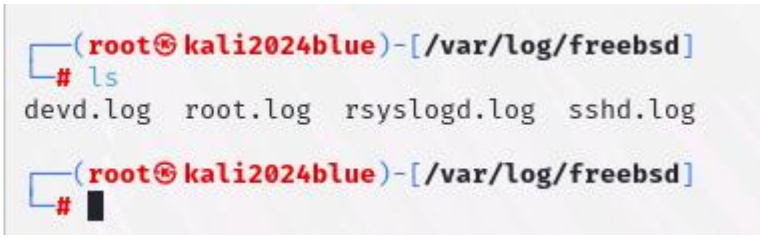
Dans le fichier /etc/rsyslog.conf du serveur de log linux



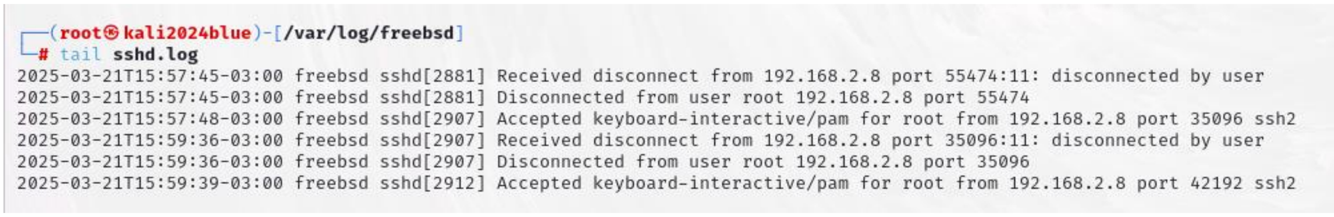
```
# /etc/rsyslog.conf configuration file for rsyslog
#
# For more information install rsyslog-doc and see
# /usr/share/doc/rsyslog-doc/html/configuration/index.html
$template RemoteLogs,"/var/log/%HOSTNAME%/%PROGRAMNAME%.log"
*.* ?RemoteLogs
& ~


#################
#### MODULES ####
#################

module(load="imuxsock") # provides support for local system logging
module(load="imklog")   # provides kernel logging support
#module(load="immark")  # provides --MARK-- message capability

# provides UDP syslog reception
#module(load="imudp")
#input(type="imudp" port="514")

# provides TCP syslog reception
module(load="imtcp")
input(type="imtcp" port="514")


###########################
#### GLOBAL DIRECTIVES ####
###########################

#
```

I

4) D´emontrez que la solution fonctionne en effectuant une connexion ssh sur la VM FreeBSD (capture ´ecran) et en montrant les logs correspondant sur le serveur de logs (captures ´ecran). (2 points)



```
┌──(root㉿kali2024blue)-[/var/log/freebsd]
└─# ls
devd.log  root.log  rsyslogd.log  sshd.log

┌──(root㉿kali2024blue)-[/var/log/freebsd]
└─# █
```

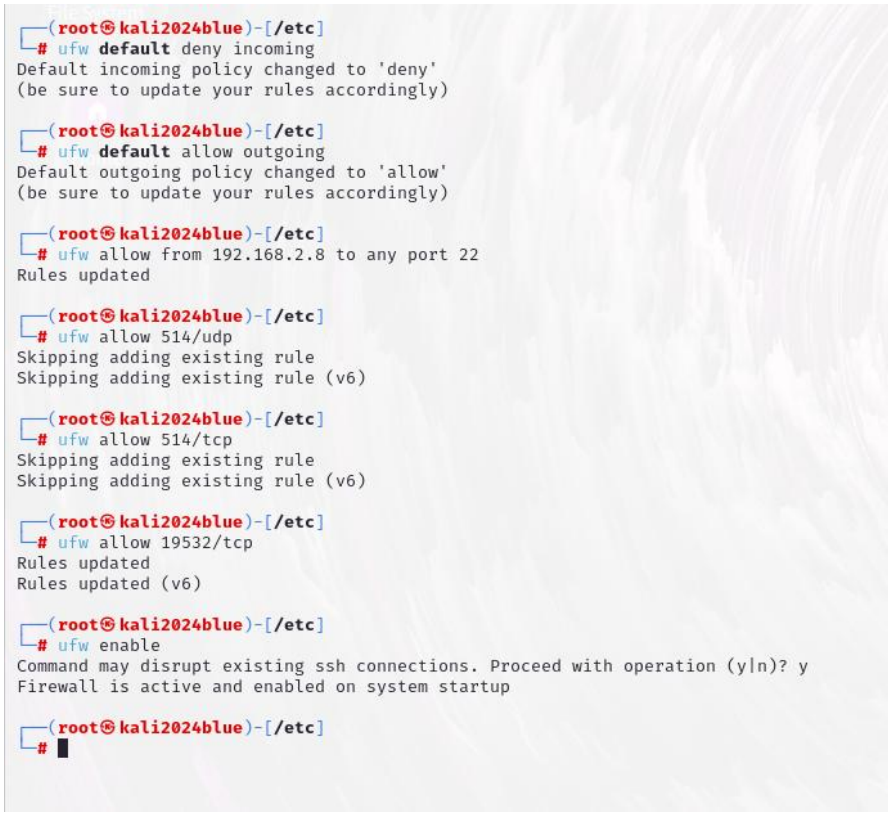


```
┌──(root㉿kali2024blue)-[/var/log/freebsd]
└─# tail sshd.log
2025-03-21T15:57:45-03:00 freebsd sshd[2881] Received disconnect from 192.168.2.8 port 55474:11: disconnected by user
2025-03-21T15:57:45-03:00 freebsd sshd[2881] Disconnected from user root 192.168.2.8 port 55474
2025-03-21T15:57:48-03:00 freebsd sshd[2907] Accepted keyboard-interactive/pam for root from 192.168.2.8 port 35096 ssh2
2025-03-21T15:59:36-03:00 freebsd sshd[2907] Received disconnect from 192.168.2.8 port 35096:11: disconnected by user
2025-03-21T15:59:36-03:00 freebsd sshd[2907] Disconnected from user root 192.168.2.8 port 35096
2025-03-21T15:59:39-03:00 freebsd sshd[2912] Accepted keyboard-interactive/pam for root from 192.168.2.8 port 42192 ssh2
```

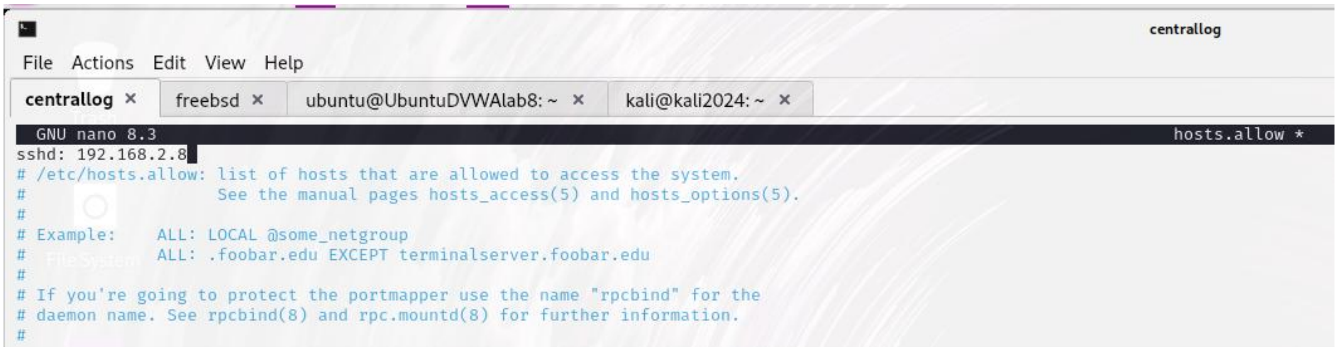
3 S´ecurisation (8 points)

L’objectif de cette partie est de s´ecuriser le syst`eme de centralisation des logs.

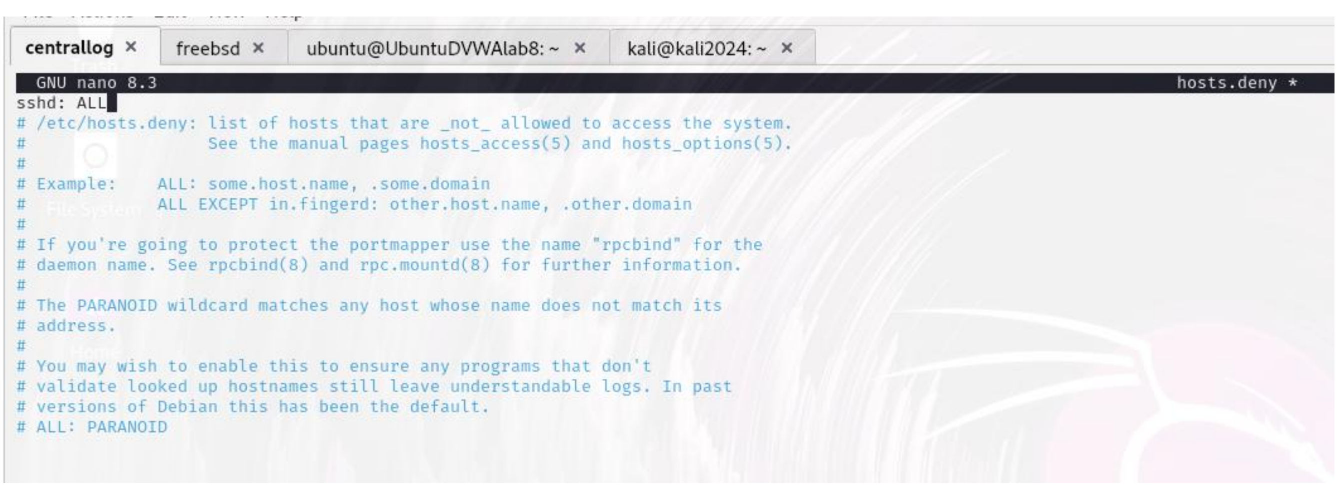
1) S´ecurisez le serveur de logs contre tous acc`es autre que la VM Kali purple. Expliquez votre solution. (1 point).



```
┌──(root㉿kali2024blue)-[/etc]
└─# ufw default deny incoming
Default incoming policy changed to 'deny'
(be sure to update your rules accordingly)

┌──(root㉿kali2024blue)-[/etc]
└─# ufw default allow outgoing
Default outgoing policy changed to 'allow'
(be sure to update your rules accordingly)

┌──(root㉿kali2024blue)-[/etc]
└─# ufw allow from 192.168.2.8 to any port 22
Rules updated

┌──(root㉿kali2024blue)-[/etc]
└─# ufw allow 514/udp
Skipping adding existing rule
Skipping adding existing rule (v6)

┌──(root㉿kali2024blue)-[/etc]
└─# ufw allow 514/tcp
Skipping adding existing rule
Skipping adding existing rule (v6)

┌──(root㉿kali2024blue)-[/etc]
└─# ufw allow 19532/tcp
Rules updated
Rules updated (v6)

┌──(root㉿kali2024blue)-[/etc]
└─# ufw enable
Command may disrupt existing ssh connections. Proceed with operation (y|n)? y
Firewall is active and enabled on system startup

┌──(root㉿kali2024blue)-[/etc]
└─# █
```

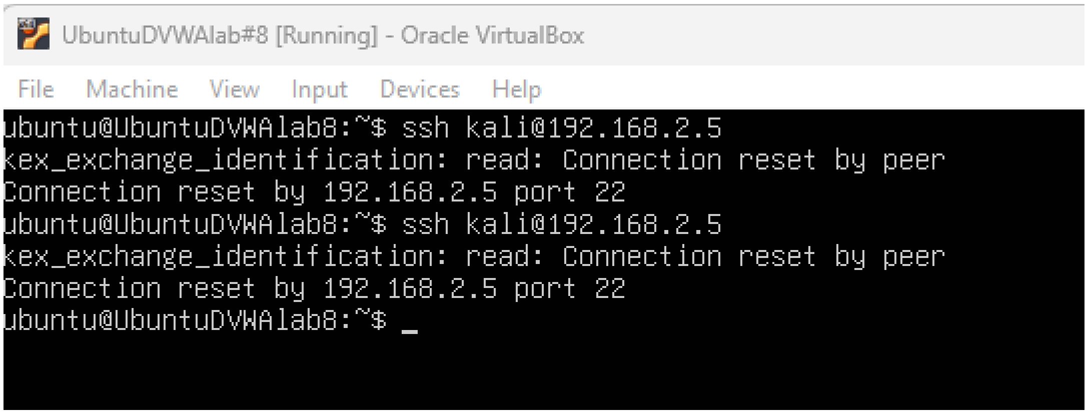


```
  GNU nano 8.3                                                                                    hosts.allow *
sshd: 192.168.2.8
# /etc/hosts.allow: list of hosts that are allowed to access the system.
#                   See the manual pages hosts_access(5) and hosts_options(5).
#
# Example:    ALL: LOCAL @some_netgroup
#             ALL: .foobar.edu EXCEPT terminalserver.foobar.edu
#
# If you're going to protect the portmapper use the name "rpcbind" for the
# daemon name. See rpcbind(8) and rpc.mountd(8) for further information.
#
```

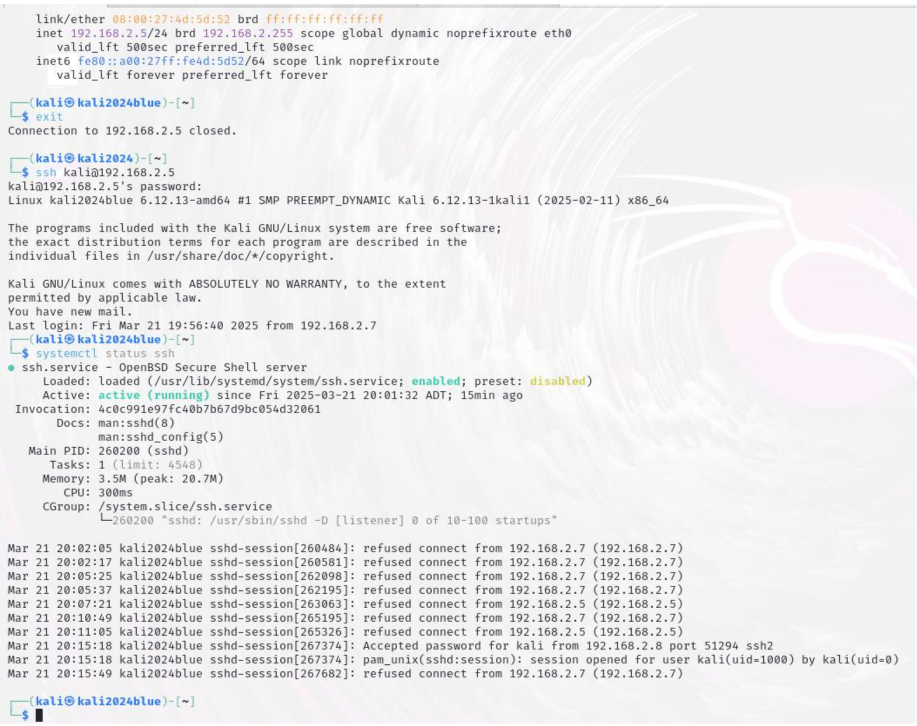


```
  GNU nano 8.3                                                                                    hosts.deny *
sshd: ALL
# /etc/hosts.deny: list of hosts that are _not_ allowed to access the system.
#                  See the manual pages hosts_access(5) and hosts_options(5).
#
# Example:    ALL: some.host.name, .some.domain
#             ALL EXCEPT in.fingerd: other.host.name, .other.domain
#
# If you're going to protect the portmapper use the name "rpcbind" for the
# daemon name. See rpcbind(8) and rpc.mountd(8) for further information.
#
# The PARANOID wildcard matches any host whose name does not match its
# address.
#
# You may wish to enable this to ensure any programs that don't
# validate looked up hostnames still leave understandable logs. In past
# versions of Debian this has been the default.
# ALL: PARANOID
```

2) D´emontrez que votre solution fonctionne a` l'aide de captures ´ecran (1 point).

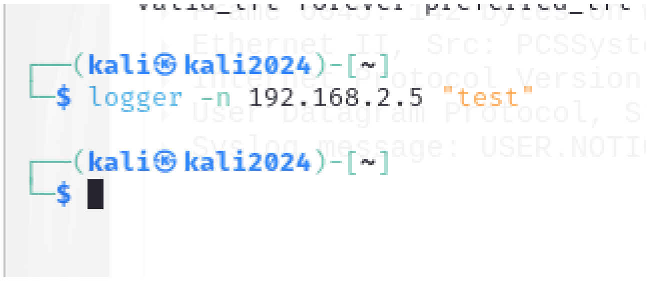

UbuntuDVWAlab#8 [Running] - Oracle VirtualBox
File Machine View Input Devices Help

```
ubuntu@UbuntuDVWAlab8:~$ ssh kali@192.168.2.5
kex_exchange_identification: read: Connection reset by peer
Connection reset by 192.168.2.5 port 22
ubuntu@UbuntuDVWAlab8:~$ ssh kali@192.168.2.5
kex_exchange_identification: read: Connection reset by peer
Connection reset by 192.168.2.5 port 22
ubuntu@UbuntuDVWAlab8:~$ _
```

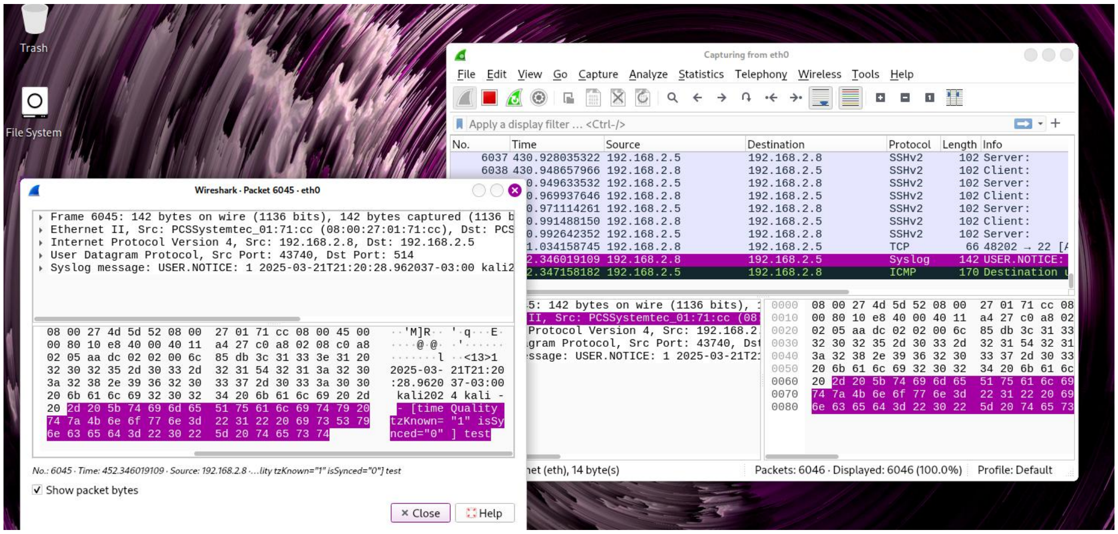


```
    link/ether 08:00:27:4d:5d:52 brd ff:ff:ff:ff:ff:ff
    inet 192.168.2.5/24 brd 192.168.2.255 scope global dynamic noprefixroute eth0
       valid_lft 500sec preferred_lft 500sec
    inet6 fe80::a00:27ff:fe4d:5d52/64 scope link noprefixroute
       valid_lft forever preferred_lft forever

┌──(kali㉿kali2024blue)-[~]
└─$ exit
Connection to 192.168.2.5 closed.

┌──(kali㉿kali2024)-[~]
└─$ ssh kali@192.168.2.5
kali@192.168.2.5's password:
Linux kali2024blue 6.12.13-amd64 #1 SMP PREEMPT_DYNAMIC Kali 6.12.13-1kali1 (2025-02-11) x86_64

The programs included with the Kali GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Kali GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
You have new mail.
Last login: Fri Mar 21 19:56:40 2025 from 192.168.2.7
┌──(kali㉿kali2024blue)-[~]
└─$ systemctl status ssh
● ssh.service - OpenBSD Secure Shell server
     Loaded: loaded (/usr/lib/systemd/system/ssh.service; enabled; preset: disabled)
     Active: active (running) since Fri 2025-03-21 20:01:32 ADT; 15min ago
 Invocation: 4c0c991e97fc40b7b67d9bc054d32061
       Docs: man:sshd(8)
             man:sshd_config(5)
   Main PID: 260200 (sshd)
      Tasks: 1 (limit: 4548)
     Memory: 3.5M (peak: 20.7M)
        CPU: 300ms
     CGroup: /system.slice/ssh.service
             └─260200 "sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups"

Mar 21 20:02:05 kali2024blue sshd-session[260484]: refused connect from 192.168.2.7 (192.168.2.7)
Mar 21 20:02:17 kali2024blue sshd-session[260581]: refused connect from 192.168.2.7 (192.168.2.7)
Mar 21 20:05:25 kali2024blue sshd-session[262098]: refused connect from 192.168.2.7 (192.168.2.7)
Mar 21 20:05:37 kali2024blue sshd-session[262195]: refused connect from 192.168.2.7 (192.168.2.7)
Mar 21 20:07:21 kali2024blue sshd-session[263063]: refused connect from 192.168.2.5 (192.168.2.5)
Mar 21 20:10:49 kali2024blue sshd-session[265195]: refused connect from 192.168.2.7 (192.168.2.7)
Mar 21 20:11:05 kali2024blue sshd-session[265326]: refused connect from 192.168.2.5 (192.168.2.5)
Mar 21 20:15:18 kali2024blue sshd-session[267374]: Accepted password for kali from 192.168.2.8 port 51294 ssh2
Mar 21 20:15:18 kali2024blue sshd-session[267374]: pam_unix(sshd:session): session opened for user kali(uid=1000) by kali(uid=0)
Mar 21 20:15:49 kali2024blue sshd-session[267682]: refused connect from 192.168.2.7 (192.168.2.7)

┌──(kali㉿kali2024blue)-[~]
└─$ █
```

3) Chiffrez la communication des logs de la VM DVWA vers le serveur de logs. Expliquer votre solution et mettez-la en place. D´emontrez que votre solution fonctionne en faisant des captures ´ecran d'un paquet IP contenant un log avec l'outil Wireshark sans le chiffrement et un autre log avec le chiffrement. (3 points).



```
┌──(kali㉿kali2024)-[~]
└─$ logger -n 192.168.2.5 "test"

┌──(kali㉿kali2024)-[~]
└─$ █
```



Trash
File System
Capturing from eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
6037	430.928035322	192.168.2.5	192.168.2.8	SSHv2	102	Server:
6038	430.948657966	192.168.2.8	192.168.2.5	SSHv2	102	Client:
	0.949633532	192.168.2.5	192.168.2.8	SSHv2	102	Server:
	0.969937646	192.168.2.8	192.168.2.5	SSHv2	102	Client:
	0.971114261	192.168.2.5	192.168.2.8	SSHv2	102	Server:
	0.991488150	192.168.2.8	192.168.2.5	SSHv2	102	Client:
	0.992642352	192.168.2.5	192.168.2.8	SSHv2	102	Server:
	1.034158745	192.168.2.8	192.168.2.5	TCP	66	48202 → 22 [A
	2.346019109	192.168.2.8	192.168.2.5	Syslog	142	USER.NOTICE:
	2.347158182	192.168.2.5	192.168.2.8	ICMP	170	Destination u

```
5: 142 bytes on wire (1136 bits), 1
II, Src: PCSSystemtec_01:71:cc (08
 Protocol Version 4, Src: 192.168.2.
gram Protocol, Src Port: 43740, Dst
ssage: USER.NOTICE: 1 2025-03-21T21
```

```
0000  08 00 27 4d 5d 52 08 00  27 01 71 cc 08
0010  00 80 10 e8 40 00 40 11  a4 27 c0 a8 02
0020  02 05 aa dc 02 02 00 6c  85 db 3c 31 33
0030  32 30 32 35 2d 30 33 2d  32 31 54 32 31
0040  3a 32 38 2e 39 36 32 30  33 37 2d 30 33
0050  20 6b 61 6c 69 32 30 32  34 20 6b 61 6c
0060  20 2d 20 5b 74 69 6d 65  51 75 61 6c 69
0070  74 7a 4b 6e 6f 77 6e 3d  22 31 22 20 69
0080  6e 63 65 64 3d 22 30 22  5d 20 74 65 73
```

net (eth), 14 byte(s) · Packets: 6046 · Displayed: 6046 (100.0%) · Profile: Default

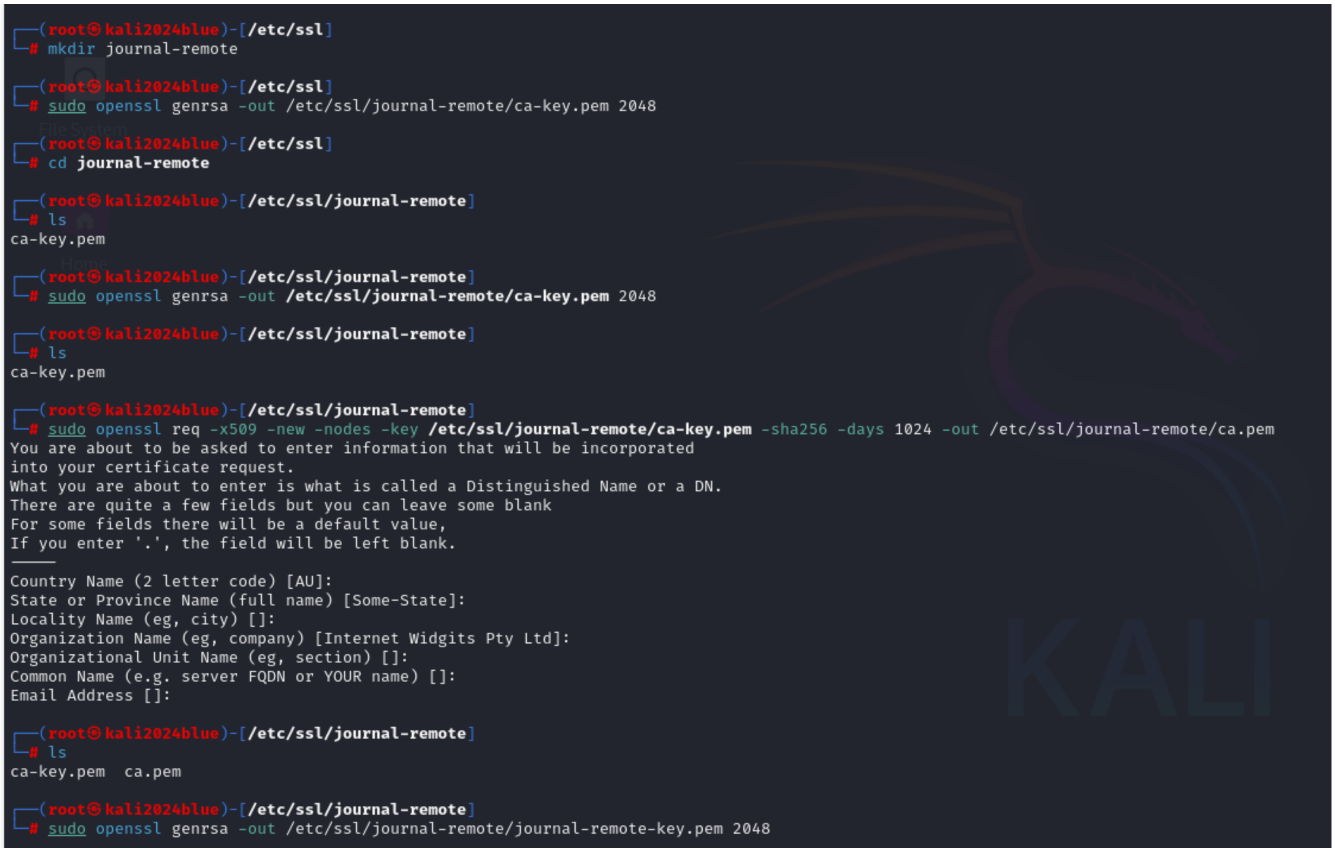
Wireshark · Packet 6045 · eth0

```
▸ Frame 6045: 142 bytes on wire (1136 bits), 142 bytes captured (1136 b
▸ Ethernet II, Src: PCSSystemtec_01:71:cc (08:00:27:01:71:cc), Dst: PCS
▸ Internet Protocol Version 4, Src: 192.168.2.8, Dst: 192.168.2.5
▸ User Datagram Protocol, Src Port: 43740, Dst Port: 514
▸ Syslog message: USER.NOTICE: 1 2025-03-21T21:20:28.962037-03:00 kali2
```

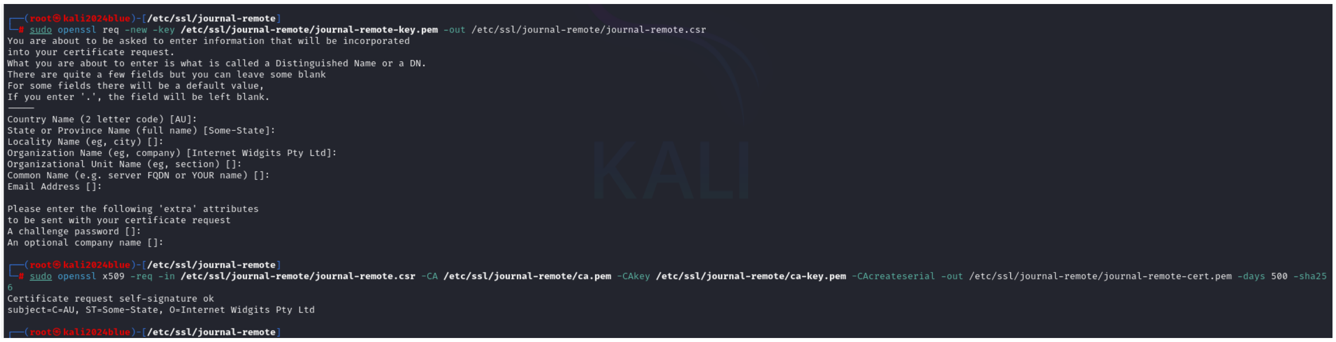
```
08 00 27 4d 5d 52 08 00  27 01 71 cc 08 00 45 00   ··'M]R·· '·q···E·
00 80 10 e8 40 00 40 11  a4 27 c0 a8 02 08 c0 a8   ····@·@· ·'······
02 05 aa dc 02 02 00 6c  85 db 3c 31 33 3e 31 20   ·······l ··<13>1
32 30 32 35 2d 30 33 2d  32 31 54 32 31 3a 32 30   2025-03- 21T21:20
3a 32 38 2e 39 36 32 30  33 37 2d 30 33 3a 30 30   :28.9620 37-03:00
20 6b 61 6c 69 32 30 32  34 20 6b 61 6c 69 20 2d    kali202 4 kali -
20 2d 20 5b 74 69 6d 65  51 75 61 6c 69 74 79 20    - [time Quality
74 7a 4b 6e 6f 77 6e 3d  22 31 22 20 69 73 53 79   tzKnown= "1" isSy
6e 63 65 64 3d 22 30 22  5d 20 74 65 73 74         nced="0" ] test
```

No.: 6045 · Time: 452.346019109 · Source: 192.168.2.8 ·…lity tzKnown="1" isSynced="0"] test

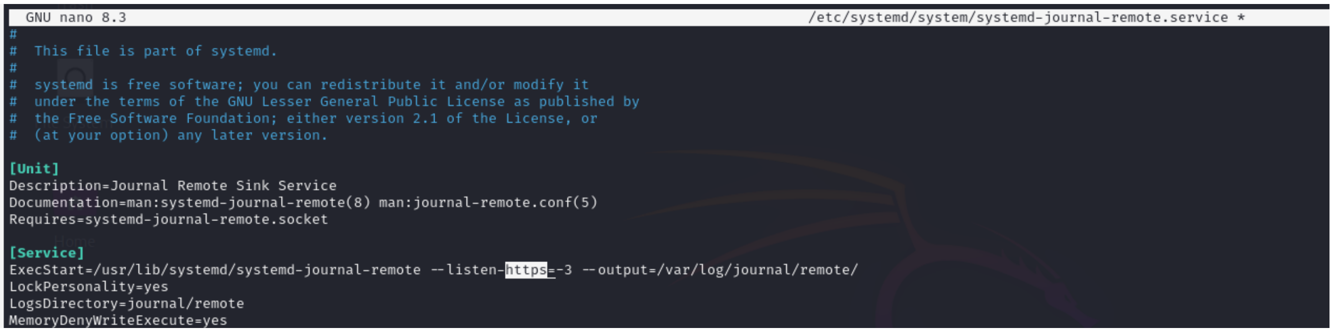
☑ Show packet bytes



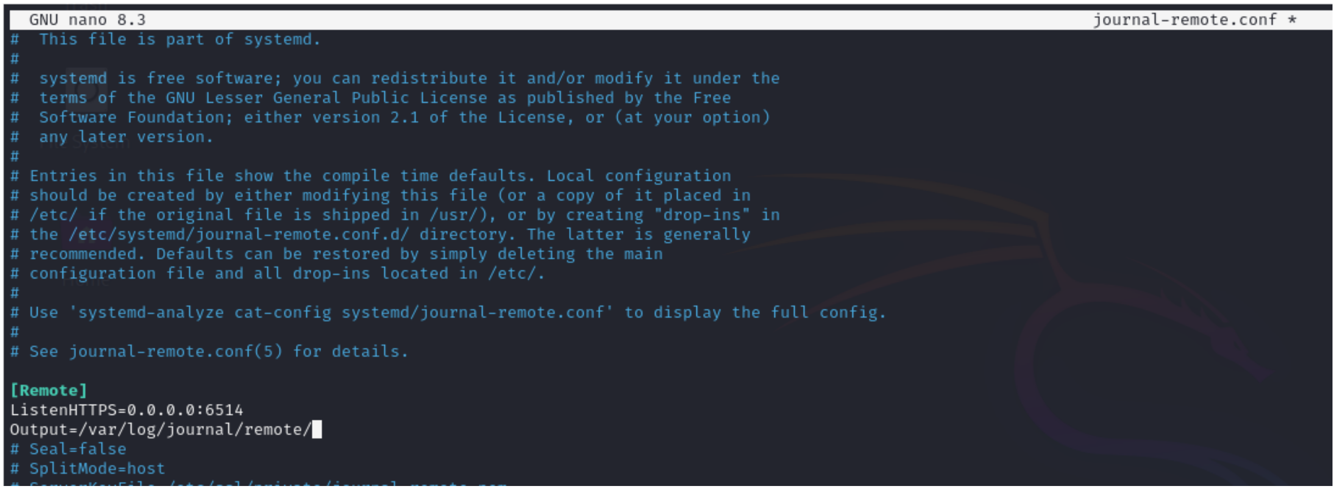
```
┌──(root㉿kali2024blue)-[/etc/ssl]
└─# mkdir journal-remote

┌──(root㉿kali2024blue)-[/etc/ssl]
└─# sudo openssl genrsa -out /etc/ssl/journal-remote/ca-key.pem 2048

┌──(root㉿kali2024blue)-[/etc/ssl]
└─# cd journal-remote

┌──(root㉿kali2024blue)-[/etc/ssl/journal-remote]
└─# ls
ca-key.pem

┌──(root㉿kali2024blue)-[/etc/ssl/journal-remote]
└─# sudo openssl genrsa -out /etc/ssl/journal-remote/ca-key.pem 2048

┌──(root㉿kali2024blue)-[/etc/ssl/journal-remote]
└─# ls
ca-key.pem

┌──(root㉿kali2024blue)-[/etc/ssl/journal-remote]
└─# sudo openssl req -x509 -new -nodes -key /etc/ssl/journal-remote/ca-key.pem -sha256 -days 1024 -out /etc/ssl/journal-remote/ca.pem
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:
State or Province Name (full name) [Some-State]:
Locality Name (eg, city) []:
Organization Name (eg, company) [Internet Widgits Pty Ltd]:
Organizational Unit Name (eg, section) []:
Common Name (e.g. server FQDN or YOUR name) []:
Email Address []:

┌──(root㉿kali2024blue)-[/etc/ssl/journal-remote]
└─# ls
ca-key.pem  ca.pem

┌──(root㉿kali2024blue)-[/etc/ssl/journal-remote]
└─# sudo openssl genrsa -out /etc/ssl/journal-remote/journal-remote-key.pem 2048
```



```
┌──(root㉿kali2024blue)-[/etc/ssl/journal-remote]
└─# sudo openssl req -new -key /etc/ssl/journal-remote/journal-remote-key.pem -out /etc/ssl/journal-remote/journal-remote.csr
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:
State or Province Name (full name) [Some-State]:
Locality Name (eg, city) []:
Organization Name (eg, company) [Internet Widgits Pty Ltd]:
Organizational Unit Name (eg, section) []:
Common Name (e.g. server FQDN or YOUR name) []:
Email Address []:

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:

┌──(root㉿kali2024blue)-[/etc/ssl/journal-remote]
└─# sudo openssl x509 -req -in /etc/ssl/journal-remote/journal-remote.csr -CA /etc/ssl/journal-remote/ca.pem -CAkey /etc/ssl/journal-remote/ca-key.pem -CAcreateserial -out /etc/ssl/journal-remote/journal-remote-cert.pem -days 500 -sha25
6
Certificate request self-signature ok
subject=C=AU, ST=Some-State, O=Internet Widgits Pty Ltd

┌──(root㉿kali2024blue)-[/etc/ssl/journal-remote]
```



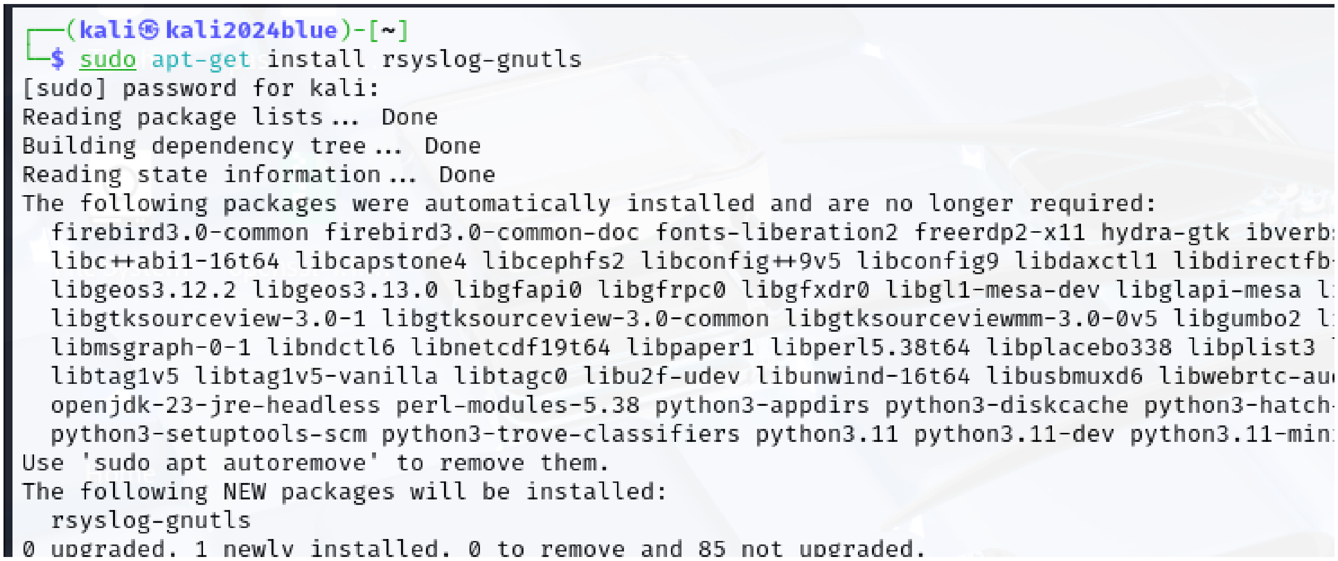
```
  GNU nano 8.3                                            /etc/systemd/system/systemd-journal-remote.service *
#
#  This file is part of systemd.
#
#  systemd is free software; you can redistribute it and/or modify it
#  under the terms of the GNU Lesser General Public License as published by
#  the Free Software Foundation; either version 2.1 of the License, or
#  (at your option) any later version.

[Unit]
Description=Journal Remote Sink Service
Documentation=man:systemd-journal-remote(8) man:journal-remote.conf(5)
Requires=systemd-journal-remote.socket

[Service]
ExecStart=/usr/lib/systemd/systemd-journal-remote --listen-https=-3 --output=/var/log/journal/remote/
LockPersonality=yes
LogsDirectory=journal/remote
MemoryDenyWriteExecute=yes
```



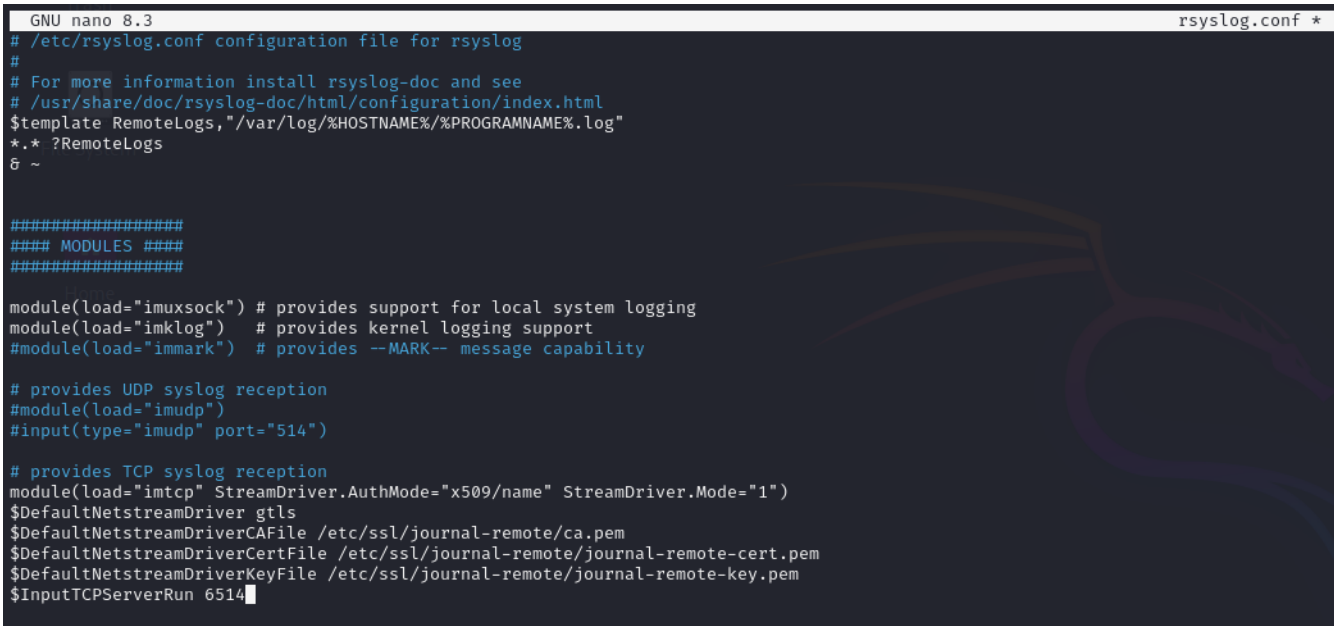
```
  GNU nano 8.3                                                                          journal-remote.conf *
#  This file is part of systemd.
#
#  systemd is free software; you can redistribute it and/or modify it under the
#  terms of the GNU Lesser General Public License as published by the Free
#  Software Foundation; either version 2.1 of the License, or (at your option)
#  any later version.
#
# Entries in this file show the compile time defaults. Local configuration
# should be created by either modifying this file (or a copy of it placed in
# /etc/ if the original file is shipped in /usr/), or by creating "drop-ins" in
# the /etc/systemd/journal-remote.conf.d/ directory. The latter is generally
# recommended. Defaults can be restored by simply deleting the main
# configuration file and all drop-ins located in /etc/.
#
# Use 'systemd-analyze cat-config systemd/journal-remote.conf' to display the full config.
#
# See journal-remote.conf(5) for details.

[Remote]
ListenHTTPS=0.0.0.0:6514
Output=/var/log/journal/remote/
# Seal=false
# SplitMode=host
# ServerKeyFile=/etc/ssl/private/journal-remote.pem
```

4) Idem que 3) mais pour la communication des logs entre VM FreeBSD vers le serveur de logs.(3 points).

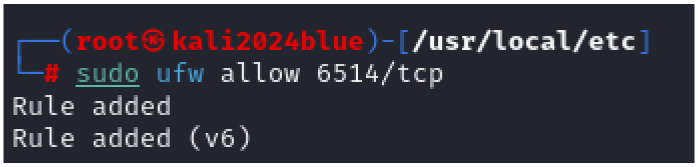
Sur le serveur de log



```
┌──(kali㉿kali2024blue)-[~]
└─$ sudo apt-get install rsyslog-gnutls
[sudo] password for kali:
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following packages were automatically installed and are no longer required:
  firebird3.0-common firebird3.0-common-doc fonts-liberation2 freerdp2-x11 hydra-gtk ibverb
  libc++abi1-16t64 libcapstone4 libcephfs2 libconfig++9v5 libconfig9 libdaxctl1 libdirectfb
  libgeos3.12.2 libgeos3.13.0 libgfapi0 libgfrpc0 libgfxdr0 libgl1-mesa-dev libglapi-mesa l
  libgtksourceview-3.0-1 libgtksourceview-3.0-common libgtksourceviewmm-3.0-0v5 libgumbo2 l
  libmsgraph-0-1 libndctl6 libnetcdf19t64 libpaper1 libperl5.38t64 libplacebo338 libplist3
  libtag1v5 libtag1v5-vanilla libtagc0 libu2f-udev libunwind-16t64 libusbmuxd6 libwebrtc-au
  openjdk-23-jre-headless perl-modules-5.38 python3-appdirs python3-diskcache python3-hatch
  python3-setuptools-scm python3-trove-classifiers python3.11 python3.11-dev python3.11-min
Use 'sudo apt autoremove' to remove them.
The following NEW packages will be installed:
  rsyslog-gnutls
0 upgraded, 1 newly installed, 0 to remove and 85 not upgraded.
```

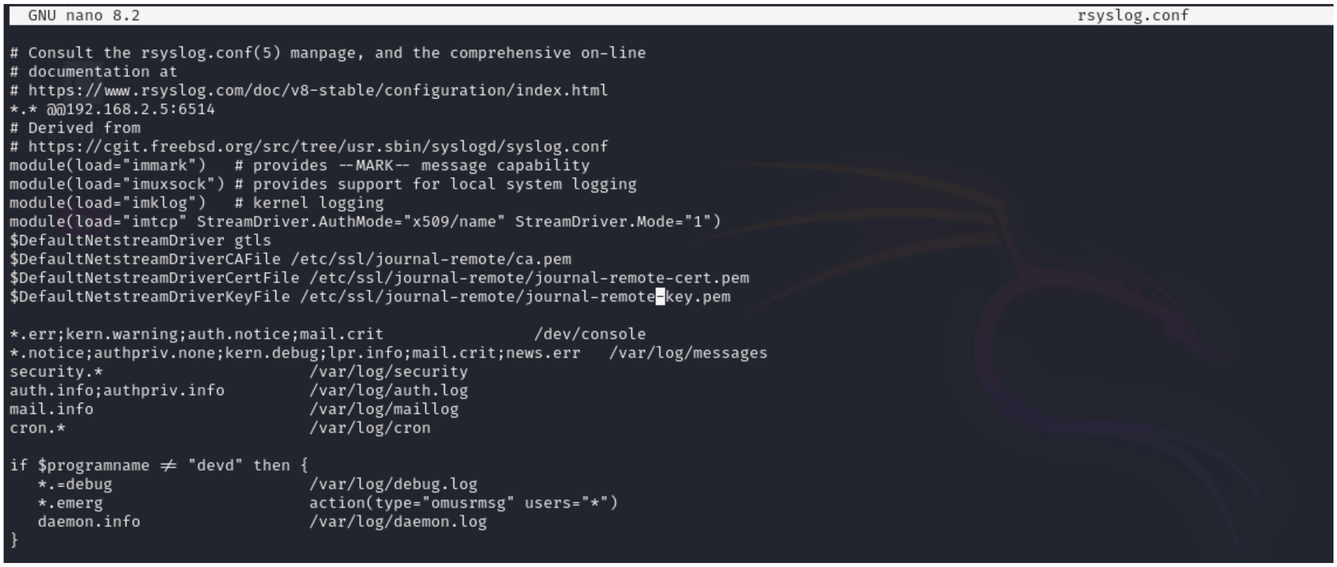


```
  GNU nano 8.3                                                                                               rsyslog.conf *
# /etc/rsyslog.conf configuration file for rsyslog
#
# For more information install rsyslog-doc and see
# /usr/share/doc/rsyslog-doc/html/configuration/index.html
$template RemoteLogs,"/var/log/%HOSTNAME%/%PROGRAMNAME%.log"
*.* ?RemoteLogs
& ~


#################
#### MODULES ####
#################

module(load="imuxsock") # provides support for local system logging
module(load="imklog")   # provides kernel logging support
#module(load="immark")  # provides --MARK-- message capability

# provides UDP syslog reception
#module(load="imudp")
#input(type="imudp" port="514")

# provides TCP syslog reception
module(load="imtcp" StreamDriver.AuthMode="x509/name" StreamDriver.Mode="1")
$DefaultNetstreamDriver gtls
$DefaultNetstreamDriverCAFile /etc/ssl/journal-remote/ca.pem
$DefaultNetstreamDriverCertFile /etc/ssl/journal-remote/journal-remote-cert.pem
$DefaultNetstreamDriverKeyFile /etc/ssl/journal-remote/journal-remote-key.pem
$InputTCPServerRun 6514
```

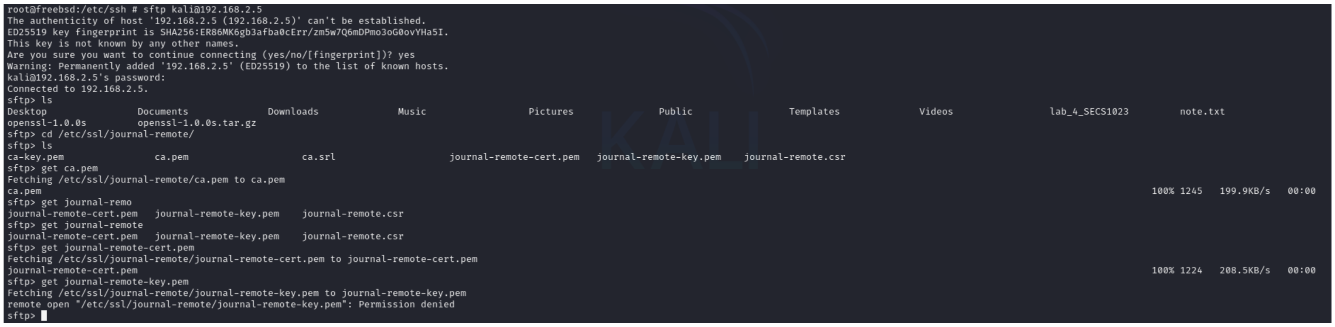


```
┌──(root㉿kali2024blue)-[/usr/local/etc]
└─# sudo ufw allow 6514/tcp
Rule added
Rule added (v6)
```

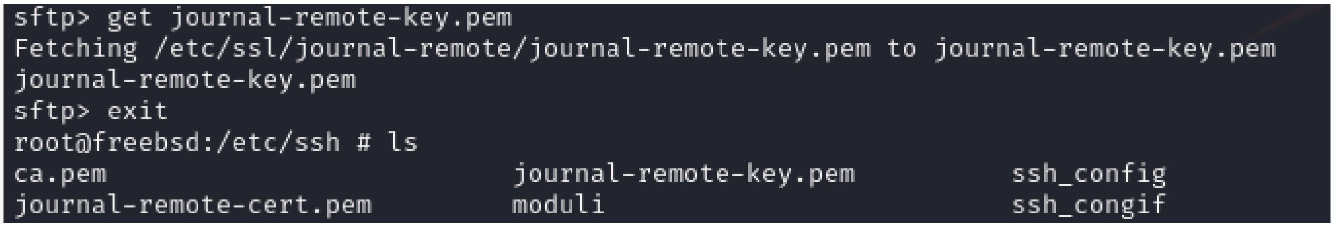
Sur la FreeBSD



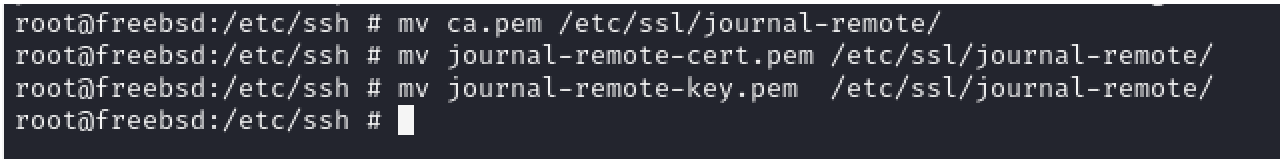
```
  GNU nano 8.2                                                                                          rsyslog.conf

# Consult the rsyslog.conf(5) manpage, and the comprehensive on-line
# documentation at
# https://www.rsyslog.com/doc/v8-stable/configuration/index.html
*.* @@192.168.2.5:6514
# Derived from
# https://cgit.freebsd.org/src/tree/usr.sbin/syslogd/syslog.conf
module(load="immark")   # provides --MARK-- message capability
module(load="imuxsock") # provides support for local system logging
module(load="imklog")   # kernel logging
module(load="imtcp" StreamDriver.AuthMode="x509/name" StreamDriver.Mode="1")
$DefaultNetstreamDriver gtls
$DefaultNetstreamDriverCAFile /etc/ssl/journal-remote/ca.pem
$DefaultNetstreamDriverCertFile /etc/ssl/journal-remote/journal-remote-cert.pem
$DefaultNetstreamDriverKeyFile /etc/ssl/journal-remote/journal-remote-key.pem

*.err;kern.warning;auth.notice;mail.crit                /dev/console
*.notice;authpriv.none;kern.debug;lpr.info;mail.crit;news.err   /var/log/messages
security.*                      /var/log/security
auth.info;authpriv.info         /var/log/auth.log
mail.info                       /var/log/maillog
cron.*                          /var/log/cron

if $programname ≠ "devd" then {
   *.=debug                     /var/log/debug.log
   *.emerg                      action(type="omusrmsg" users="*")
   daemon.info                  /var/log/daemon.log
}
```



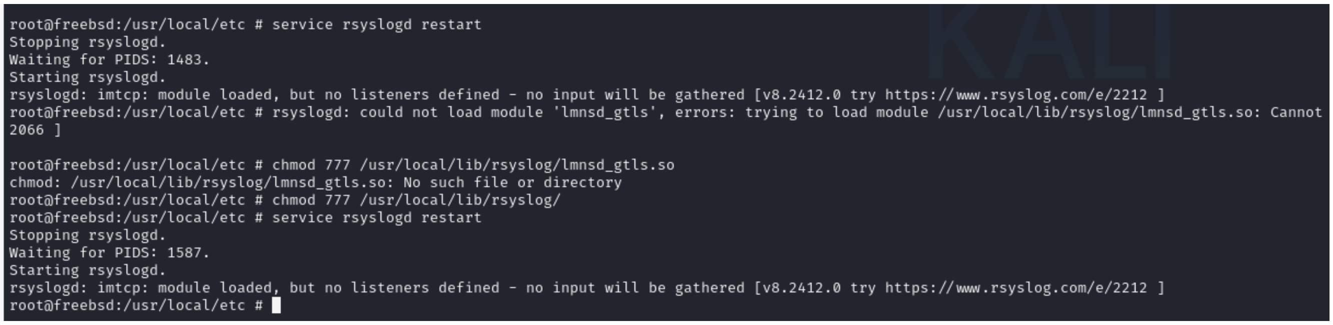
```
root@freebsd:/etc/ssh # sftp kali@192.168.2.5
The authenticity of host '192.168.2.5 (192.168.2.5)' can't be established.
ED25519 key fingerprint is SHA256:ER86MK6gb3afba0cErr/zm5w7Q6mDPmo3oG0ovYHa5I.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.2.5' (ED25519) to the list of known hosts.
kali@192.168.2.5's password:
Connected to 192.168.2.5.
sftp> ls
Desktop              Documents            Downloads            Music                Pictures             Public               Templates            Videos               lab_4_SECS1023       note.txt
openssl-1.0.0s       openssl-1.0.0s.tar.gz
sftp> cd /etc/ssl/journal-remote/
sftp> ls
ca-key.pem              ca.pem                  ca.srl                  journal-remote-cert.pem   journal-remote-key.pem    journal-remote.csr
sftp> get ca.pem
Fetching /etc/ssl/journal-remote/ca.pem to ca.pem
ca.pem                                                                                                          100% 1245   199.9KB/s   00:00
sftp> get journal-remo
journal-remote-cert.pem   journal-remote-key.pem    journal-remote.csr
sftp> get journal-remote
journal-remote-cert.pem   journal-remote-key.pem    journal-remote.csr
sftp> get journal-remote-cert.pem
Fetching /etc/ssl/journal-remote/journal-remote-cert.pem to journal-remote-cert.pem
journal-remote-cert.pem                                                                                         100% 1224   208.5KB/s   00:00
sftp> get journal-remote-key.pem
Fetching /etc/ssl/journal-remote/journal-remote-key.pem to journal-remote-key.pem
remote open "/etc/ssl/journal-remote/journal-remote-key.pem": Permission denied
sftp> 
```



```
sftp> get journal-remote-key.pem
Fetching /etc/ssl/journal-remote/journal-remote-key.pem to journal-remote-key.pem
journal-remote-key.pem
sftp> exit
root@freebsd:/etc/ssh # ls
ca.pem                          journal-remote-key.pem          ssh_config
journal-remote-cert.pem         moduli                          ssh_congif
```

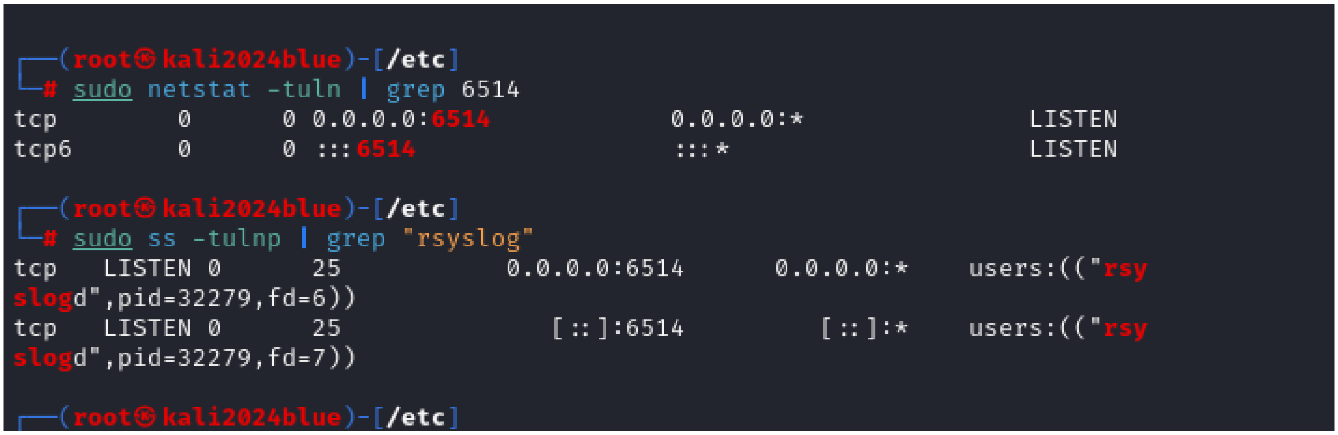


```
root@freebsd:/etc/ssh # mv ca.pem /etc/ssl/journal-remote/
root@freebsd:/etc/ssh # mv journal-remote-cert.pem /etc/ssl/journal-remote/
root@freebsd:/etc/ssh # mv journal-remote-key.pem  /etc/ssl/journal-remote/
root@freebsd:/etc/ssh # 
```

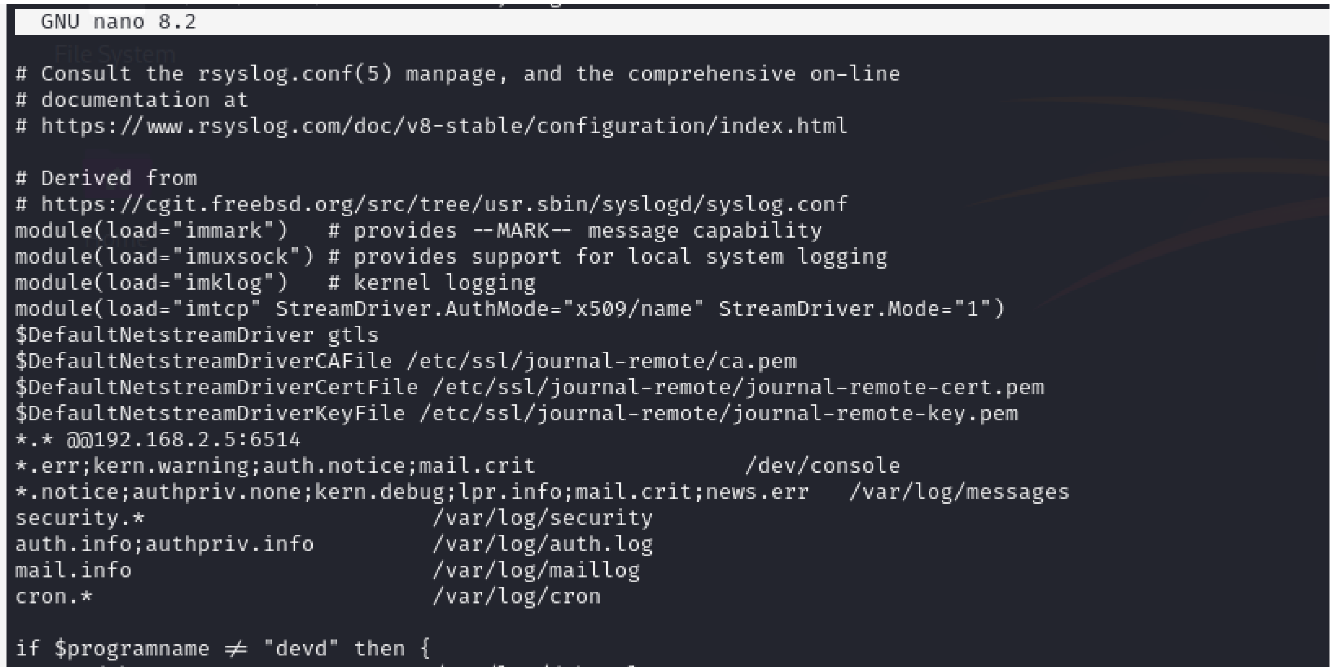


```
root@freebsd:/usr/local/etc # service rsyslogd restart
Stopping rsyslogd.
Waiting for PIDS: 1483.
Starting rsyslogd.
rsyslogd: imtcp: module loaded, but no listeners defined - no input will be gathered [v8.2412.0 try https://www.rsyslog.com/e/2212 ]
root@freebsd:/usr/local/etc # rsyslogd: could not load module 'lmnsd_gtls', errors: trying to load module /usr/local/lib/rsyslog/lmnsd_gtls.so: Cannot
2066 ]

root@freebsd:/usr/local/etc # chmod 777 /usr/local/lib/rsyslog/lmnsd_gtls.so
chmod: /usr/local/lib/rsyslog/lmnsd_gtls.so: No such file or directory
root@freebsd:/usr/local/etc # chmod 777 /usr/local/lib/rsyslog/
root@freebsd:/usr/local/etc # service rsyslogd restart
Stopping rsyslogd.
Waiting for PIDS: 1587.
Starting rsyslogd.
rsyslogd: imtcp: module loaded, but no listeners defined - no input will be gathered [v8.2412.0 try https://www.rsyslog.com/e/2212 ]
root@freebsd:/usr/local/etc # 
```

Même si jai activer mon listener ca ne fonctionne pas



```
┌──(root㉿kali2024blue)-[/etc]
└─# sudo netstat -tuln | grep 6514
tcp        0      0 0.0.0.0:6514            0.0.0.0:*               LISTEN
tcp6       0      0 :::6514                 :::*                    LISTEN

┌──(root㉿kali2024blue)-[/etc]
└─# sudo ss -tulnp | grep "rsyslog"
tcp   LISTEN 0      25           0.0.0.0:6514       0.0.0.0:*    users:(("rsy
slogd",pid=32279,fd=6))
tcp   LISTEN 0      25              [::]:6514          [::]:*    users:(("rsy
slogd",pid=32279,fd=7))

┌──(root㉿kali2024blue)-[/etc]
```

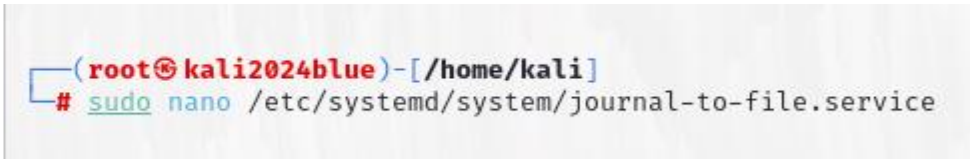


```
  GNU nano 8.2

# Consult the rsyslog.conf(5) manpage, and the comprehensive on-line
# documentation at
# https://www.rsyslog.com/doc/v8-stable/configuration/index.html

# Derived from
# https://cgit.freebsd.org/src/tree/usr.sbin/syslogd/syslog.conf
module(load="immark")   # provides --MARK-- message capability
module(load="imuxsock") # provides support for local system logging
module(load="imklog")   # kernel logging
module(load="imtcp" StreamDriver.AuthMode="x509/name" StreamDriver.Mode="1")
$DefaultNetstreamDriver gtls
$DefaultNetstreamDriverCAFile /etc/ssl/journal-remote/ca.pem
$DefaultNetstreamDriverCertFile /etc/ssl/journal-remote/journal-remote-cert.pem
$DefaultNetstreamDriverKeyFile /etc/ssl/journal-remote/journal-remote-key.pem
*.* @@192.168.2.5:6514
*.err;kern.warning;auth.notice;mail.crit                /dev/console
*.notice;authpriv.none;kern.debug;lpr.info;mail.crit;news.err   /var/log/messages
security.*                      /var/log/security
auth.info;authpriv.info         /var/log/auth.log
mail.info                       /var/log/maillog
cron.*                          /var/log/cron

if $programname ≠ "devd" then {
```

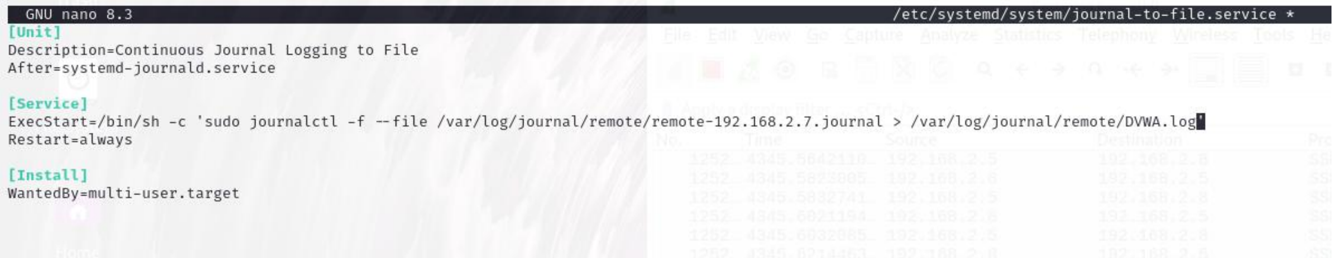
4 Surveillance/Monitoring (4 points)

L'objectif de cette partie est d'utiliser la VM Kali purple comme syst`eme d'affichage/visualisation des logs centralis´es de la VM Serveur-logs.

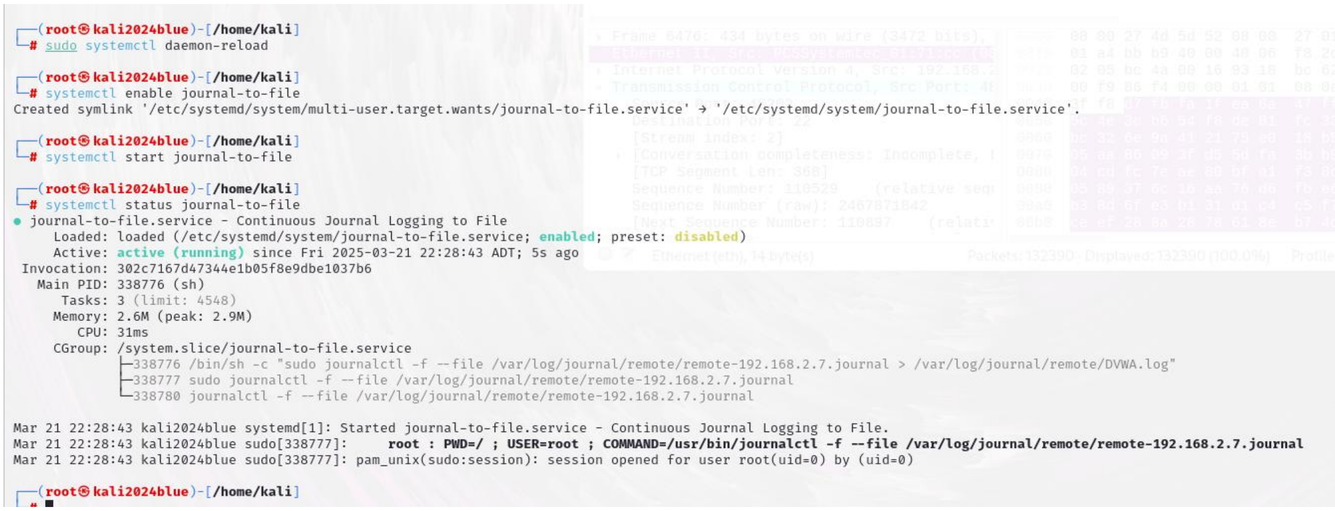
Créer un service qui transfert le contenu de mon dossier .journal en dossier log pour être en mesure d'ouvrir les deux machines dans la même application.



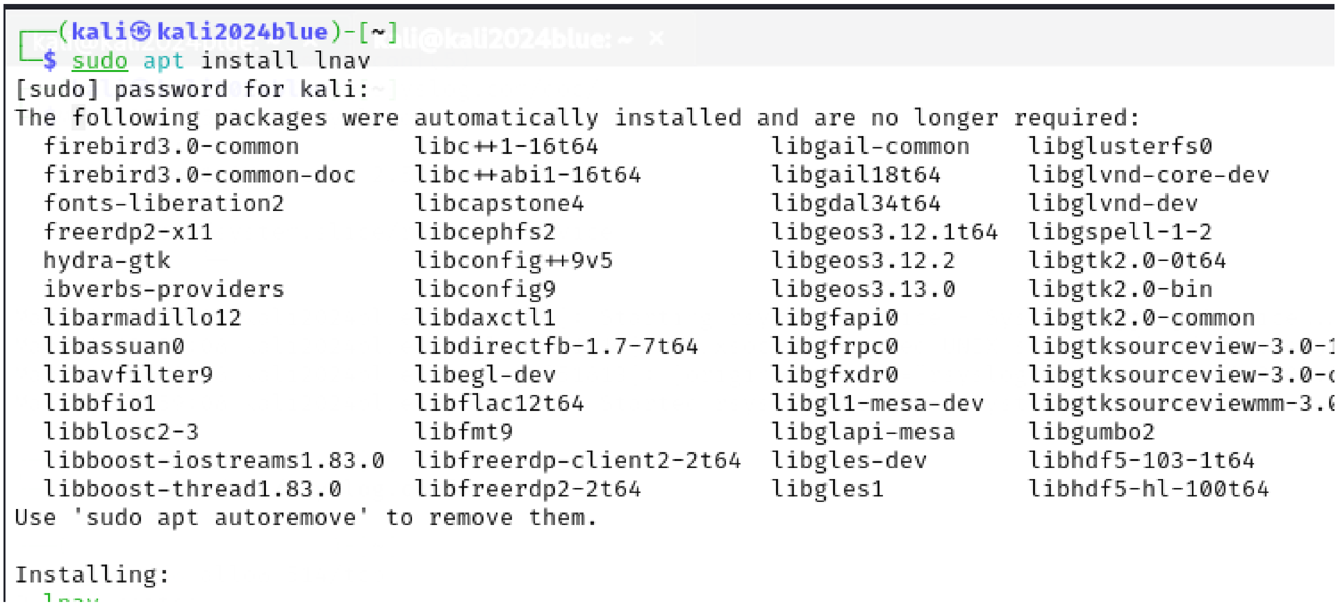
```
┌──(root㉿kali2024blue)-[/home/kali]
└─# sudo nano /etc/systemd/system/journal-to-file.service
```



```
  GNU nano 8.3                                          /etc/systemd/system/journal-to-file.service *
[Unit]
Description=Continuous Journal Logging to File
After=systemd-journald.service

[Service]
ExecStart=/bin/sh -c 'sudo journalctl -f --file /var/log/journal/remote/remote-192.168.2.7.journal > /var/log/journal/remote/DVWA.log'
Restart=always

[Install]
WantedBy=multi-user.target
```



```
┌──(root㉿kali2024blue)-[/home/kali]
└─# sudo systemctl daemon-reload

┌──(root㉿kali2024blue)-[/home/kali]
└─# systemctl enable journal-to-file
Created symlink '/etc/systemd/system/multi-user.target.wants/journal-to-file.service' → '/etc/systemd/system/journal-to-file.service'.

┌──(root㉿kali2024blue)-[/home/kali]
└─# systemctl start journal-to-file

┌──(root㉿kali2024blue)-[/home/kali]
└─# systemctl status journal-to-file
● journal-to-file.service - Continuous Journal Logging to File
     Loaded: loaded (/etc/systemd/system/journal-to-file.service; enabled; preset: disabled)
     Active: active (running) since Fri 2025-03-21 22:28:43 ADT; 5s ago
 Invocation: 302c7167d47344e1b05f8e9dbe1037b6
   Main PID: 338776 (sh)
      Tasks: 3 (limit: 4548)
     Memory: 2.6M (peak: 2.9M)
        CPU: 31ms
     CGroup: /system.slice/journal-to-file.service
             ├─338776 /bin/sh -c "sudo journalctl -f --file /var/log/journal/remote/remote-192.168.2.7.journal > /var/log/journal/remote/DVWA.log"
             ├─338777 sudo journalctl -f --file /var/log/journal/remote/remote-192.168.2.7.journal
             └─338780 journalctl -f --file /var/log/journal/remote/remote-192.168.2.7.journal

Mar 21 22:28:43 kali2024blue systemd[1]: Started journal-to-file.service - Continuous Journal Logging to File.
Mar 21 22:28:43 kali2024blue sudo[338777]:     root : PWD=/ ; USER=root ; COMMAND=/usr/bin/journalctl -f --file /var/log/journal/remote/remote-192.168.2.7.journal
Mar 21 22:28:43 kali2024blue sudo[338777]: pam_unix(sudo:session): session opened for user root(uid=0) by (uid=0)

┌──(root㉿kali2024blue)-[/home/kali]
└─# █
```

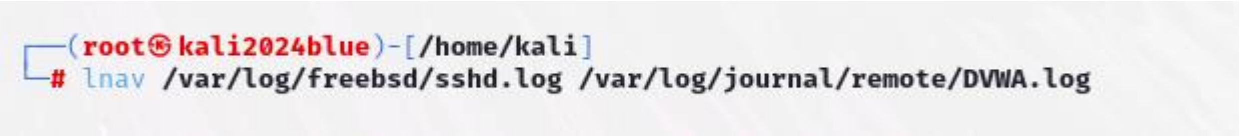


```
┌──(kali㉿kali2024blue)-[~]
└─$ sudo apt install lnav
[sudo] password for kali:
The following packages were automatically installed and are no longer required:
  firebird3.0-common        libc++1-16t64             libgail-common     libglusterfs0
  firebird3.0-common-doc    libc++abi1-16t64          libgail18t64       libglvnd-core-dev
  fonts-liberation2         libcapstone4              libgdal34t64       libglvnd-dev
  freerdp2-x11              libcephfs2                libgeos3.12.1t64   libgspell-1-2
  hydra-gtk                 libconfig++9v5            libgeos3.12.2      libgtk2.0-0t64
  ibverbs-providers         libconfig9                libgeos3.13.0      libgtk2.0-bin
  libarmadillo12            libdaxctl1                libgfapi0          libgtk2.0-common
  libassuan0                libdirectfb-1.7-7t64      libgfrpc0          libgtksourceview-3.0-1
  libavfilter9              libegl-dev                libgfxdr0          libgtksourceview-3.0-c
  libbfio1                  libflac12t64              libgl1-mesa-dev    libgtksourceviewmm-3.0
  libblosc2-3               libfmt9                   libglapi-mesa      libgumbo2
  libboost-iostreams1.83.0  libfreerdp-client2-2t64   libgles-dev        libhdf5-103-1t64
  libboost-thread1.83.0     libfreerdp2-2t64          libgles1           libhdf5-hl-100t64
Use 'sudo apt autoremove' to remove them.

Installing:
  lnav
```

1) D´ecrivez la solution (l’outil) que vous avez choisie pour visualiser les logs centralis´es a` l’aide d’explications textuelles et de captures ´ecran. (1 point)

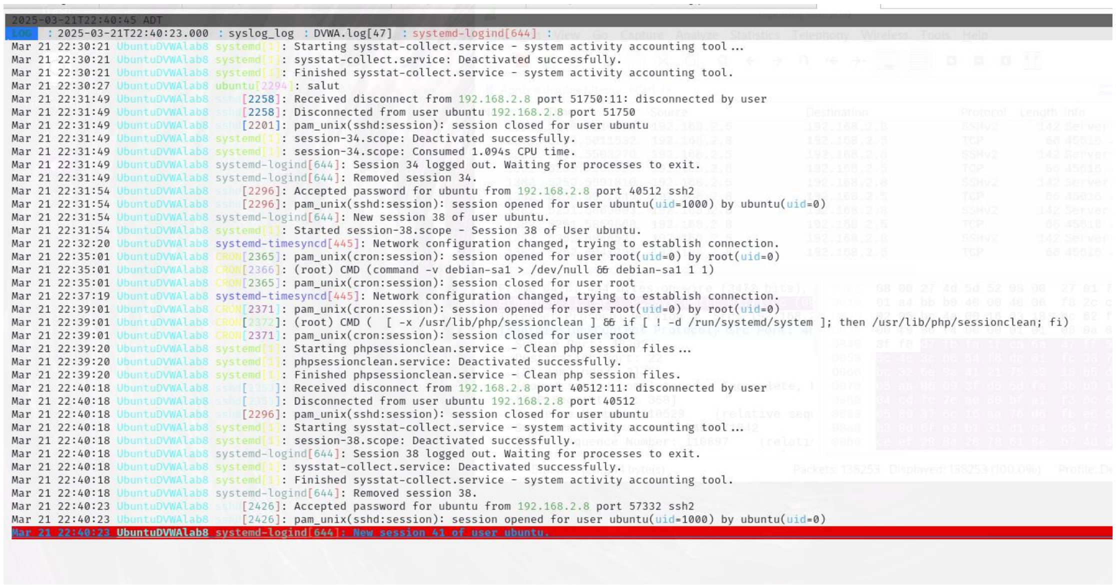
C’est tout simplement une application qui affiche les logs.

Lnav avec les deux fichiers en ligne de commande.



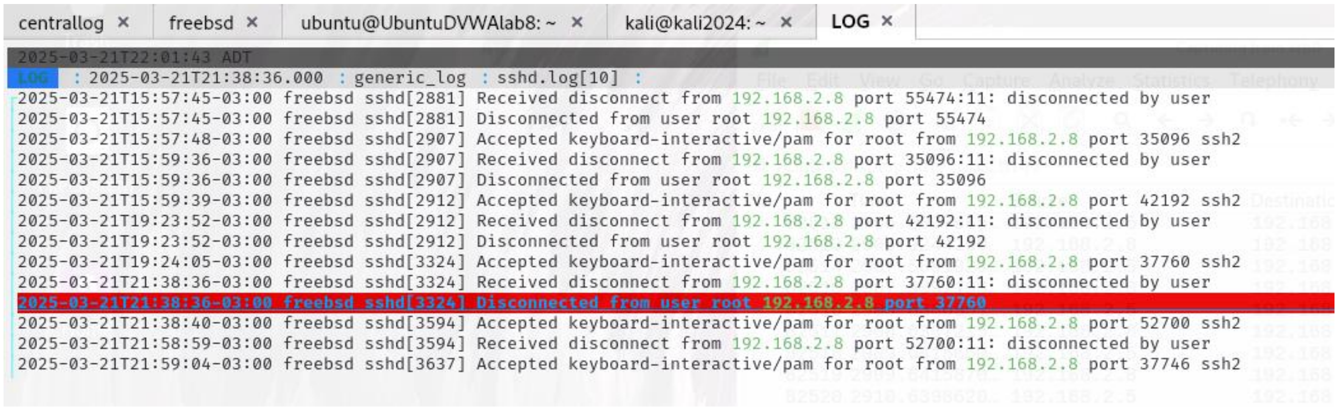
```
┌──(root㉿kali2024blue)-[/home/kali]
└─# lnav /var/log/freebsd/sshd.log /var/log/journal/remote/DVWA.log
```

2) Avec votre solution, affichez les logs de connexion ssh de la VM DVWA (capture ´ecran) (1 point)



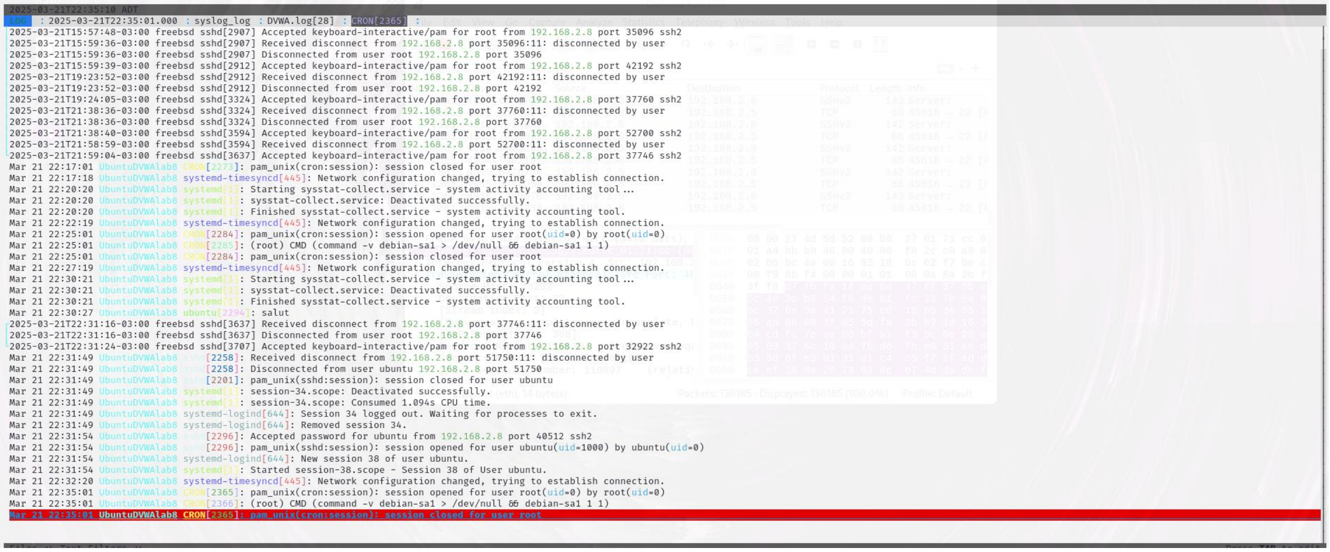
```
2025-03-21T22:40:45 ADT
LOG  : 2025-03-21T22:40:23.000  : syslog_log  : DVWA.log[47]  : systemd-logind[644]  :
Mar 21 22:30:21 UbuntuDVWAlab8 systemd[1]: Starting sysstat-collect.service - system activity accounting tool...
Mar 21 22:30:21 UbuntuDVWAlab8 systemd[1]: sysstat-collect.service: Deactivated successfully.
Mar 21 22:30:21 UbuntuDVWAlab8 systemd[1]: Finished sysstat-collect.service - system activity accounting tool.
Mar 21 22:30:27 UbuntuDVWAlab8 ubuntu[2294]: salut
Mar 21 22:31:49 UbuntuDVWAlab8 sshd[2258]: Received disconnect from 192.168.2.8 port 51750:11: disconnected by user
Mar 21 22:31:49 UbuntuDVWAlab8 sshd[2258]: Disconnected from user ubuntu 192.168.2.8 port 51750
Mar 21 22:31:49 UbuntuDVWAlab8 sshd[2201]: pam_unix(sshd:session): session closed for user ubuntu
Mar 21 22:31:49 UbuntuDVWAlab8 systemd[1]: session-34.scope: Deactivated successfully.
Mar 21 22:31:49 UbuntuDVWAlab8 systemd[1]: session-34.scope: Consumed 1.094s CPU time.
Mar 21 22:31:49 UbuntuDVWAlab8 systemd-logind[644]: Session 34 logged out. Waiting for processes to exit.
Mar 21 22:31:49 UbuntuDVWAlab8 systemd-logind[644]: Removed session 34.
Mar 21 22:31:54 UbuntuDVWAlab8 sshd[2296]: Accepted password for ubuntu from 192.168.2.8 port 40512 ssh2
Mar 21 22:31:54 UbuntuDVWAlab8 sshd[2296]: pam_unix(sshd:session): session opened for user ubuntu(uid=1000) by ubuntu(uid=0)
Mar 21 22:31:54 UbuntuDVWAlab8 systemd-logind[644]: New session 38 of user ubuntu.
Mar 21 22:31:54 UbuntuDVWAlab8 systemd[1]: Started session-38.scope - Session 38 of User ubuntu.
Mar 21 22:32:20 UbuntuDVWAlab8 systemd-timesyncd[445]: Network configuration changed, trying to establish connection.
Mar 21 22:35:01 UbuntuDVWAlab8 CRON[2365]: pam_unix(cron:session): session opened for user root(uid=0) by root(uid=0)
Mar 21 22:35:01 UbuntuDVWAlab8 CRON[2366]: (root) CMD (command -v debian-sa1 > /dev/null && debian-sa1 1 1)
Mar 21 22:35:01 UbuntuDVWAlab8 CRON[2365]: pam_unix(cron:session): session closed for user root
Mar 21 22:37:19 UbuntuDVWAlab8 systemd-timesyncd[445]: Network configuration changed, trying to establish connection.
Mar 21 22:39:01 UbuntuDVWAlab8 CRON[2371]: pam_unix(cron:session): session opened for user root(uid=0) by root(uid=0)
Mar 21 22:39:01 UbuntuDVWAlab8 CRON[2372]: (root) CMD (  [ -x /usr/lib/php/sessionclean ] && if [ ! -d /run/systemd/system ]; then /usr/lib/php/sessionclean; fi)
Mar 21 22:39:01 UbuntuDVWAlab8 CRON[2371]: pam_unix(cron:session): session closed for user root
Mar 21 22:39:20 UbuntuDVWAlab8 systemd[1]: Starting phpsessionclean.service - Clean php session files...
Mar 21 22:39:20 UbuntuDVWAlab8 systemd[1]: phpsessionclean.service: Deactivated successfully.
Mar 21 22:39:20 UbuntuDVWAlab8 systemd[1]: Finished phpsessionclean.service - Clean php session files.
Mar 21 22:40:18 UbuntuDVWAlab8 sshd[2353]: Received disconnect from 192.168.2.8 port 40512:11: disconnected by user
Mar 21 22:40:18 UbuntuDVWAlab8 sshd[2353]: Disconnected from user ubuntu 192.168.2.8 port 40512
Mar 21 22:40:18 UbuntuDVWAlab8 sshd[2296]: pam_unix(sshd:session): session closed for user ubuntu
Mar 21 22:40:18 UbuntuDVWAlab8 systemd[1]: Starting sysstat-collect.service - system activity accounting tool...
Mar 21 22:40:18 UbuntuDVWAlab8 systemd[1]: session-38.scope: Deactivated successfully.
Mar 21 22:40:18 UbuntuDVWAlab8 systemd-logind[644]: Session 38 logged out. Waiting for processes to exit.
Mar 21 22:40:18 UbuntuDVWAlab8 systemd[1]: sysstat-collect.service: Deactivated successfully.
Mar 21 22:40:18 UbuntuDVWAlab8 systemd[1]: Finished sysstat-collect.service - system activity accounting tool.
Mar 21 22:40:18 UbuntuDVWAlab8 systemd-logind[644]: Removed session 38.
Mar 21 22:40:23 UbuntuDVWAlab8 sshd[2426]: Accepted password for ubuntu from 192.168.2.8 port 57332 ssh2
Mar 21 22:40:23 UbuntuDVWAlab8 sshd[2426]: pam_unix(sshd:session): session opened for user ubuntu(uid=1000) by ubuntu(uid=0)
Mar 21 22:40:23 UbuntuDVWAlab8 systemd-logind[644]: New session 41 of user ubuntu.
```

3) Avec votre solution, affichez les logs de connexion ssh de la VM FreeBSD (capture ´ecran).(1 point)



```
2025-03-21T22:01:43 ADT
LOG  : 2025-03-21T21:38:36.000  : generic_log  : sshd.log[10]  :
2025-03-21T15:57:45-03:00 freebsd sshd[2881] Received disconnect from 192.168.2.8 port 55474:11: disconnected by user
2025-03-21T15:57:45-03:00 freebsd sshd[2881] Disconnected from user root 192.168.2.8 port 55474
2025-03-21T15:57:48-03:00 freebsd sshd[2907] Accepted keyboard-interactive/pam for root from 192.168.2.8 port 35096 ssh2
2025-03-21T15:59:36-03:00 freebsd sshd[2907] Received disconnect from 192.168.2.8 port 35096:11: disconnected by user
2025-03-21T15:59:36-03:00 freebsd sshd[2907] Disconnected from user root 192.168.2.8 port 35096
2025-03-21T15:59:39-03:00 freebsd sshd[2912] Accepted keyboard-interactive/pam for root from 192.168.2.8 port 42192 ssh2
2025-03-21T19:23:52-03:00 freebsd sshd[2912] Received disconnect from 192.168.2.8 port 42192:11: disconnected by user
2025-03-21T19:23:52-03:00 freebsd sshd[2912] Disconnected from user root 192.168.2.8 port 42192
2025-03-21T19:24:05-03:00 freebsd sshd[3324] Accepted keyboard-interactive/pam for root from 192.168.2.8 port 37760 ssh2
2025-03-21T21:38:36-03:00 freebsd sshd[3324] Received disconnect from 192.168.2.8 port 37760:11: disconnected by user
2025-03-21T21:38:36-03:00 freebsd sshd[3324] Disconnected from user root 192.168.2.8 port 37760
2025-03-21T21:38:40-03:00 freebsd sshd[3594] Accepted keyboard-interactive/pam for root from 192.168.2.8 port 52700 ssh2
2025-03-21T21:58:59-03:00 freebsd sshd[3594] Received disconnect from 192.168.2.8 port 52700:11: disconnected by user
2025-03-21T21:59:04-03:00 freebsd sshd[3637] Accepted keyboard-interactive/pam for root from 192.168.2.8 port 37746 ssh2
```

4) Avec votre solution, affichez tous les logs de DVWA et FreeBSD en tant r´eel (captures ´ecran). (1 point)



```
2025-03-21T22:35:10 ADT
LOG  : 2025-03-21T22:35:01.000  : syslog_log  : DVWA.log[28]  : CRON[2365]  :
2025-03-21T15:57:48-03:00 freebsd sshd[2907] Accepted keyboard-interactive/pam for root from 192.168.2.8 port 35096 ssh2
2025-03-21T15:59:36-03:00 freebsd sshd[2907] Received disconnect from 192.168.2.8 port 35096:11: disconnected by user
2025-03-21T15:59:36-03:00 freebsd sshd[2907] Disconnected from user root 192.168.2.8 port 35096
2025-03-21T15:59:39-03:00 freebsd sshd[2912] Accepted keyboard-interactive/pam for root from 192.168.2.8 port 42192 ssh2
2025-03-21T19:23:52-03:00 freebsd sshd[2912] Received disconnect from 192.168.2.8 port 42192:11: disconnected by user
2025-03-21T19:23:52-03:00 freebsd sshd[2912] Disconnected from user root 192.168.2.8 port 42192
2025-03-21T19:24:05-03:00 freebsd sshd[3324] Accepted keyboard-interactive/pam for root from 192.168.2.8 port 37760 ssh2
2025-03-21T21:38:36-03:00 freebsd sshd[3324] Received disconnect from 192.168.2.8 port 37760:11: disconnected by user
2025-03-21T21:38:36-03:00 freebsd sshd[3324] Disconnected from user root 192.168.2.8 port 37760
2025-03-21T21:38:40-03:00 freebsd sshd[3594] Accepted keyboard-interactive/pam for root from 192.168.2.8 port 52700 ssh2
2025-03-21T21:58:59-03:00 freebsd sshd[3594] Received disconnect from 192.168.2.8 port 52700:11: disconnected by user
2025-03-21T21:59:04-03:00 freebsd sshd[3637] Accepted keyboard-interactive/pam for root from 192.168.2.8 port 37746 ssh2
Mar 21 22:17:01 UbuntuDVWAlab8 CRON[2273]: pam_unix(cron:session): session closed for user root
Mar 21 22:17:18 UbuntuDVWAlab8 systemd-timesyncd[445]: Network configuration changed, trying to establish connection.
Mar 21 22:20:20 UbuntuDVWAlab8 systemd[1]: Starting sysstat-collect.service - system activity accounting tool…
Mar 21 22:20:20 UbuntuDVWAlab8 systemd[1]: sysstat-collect.service: Deactivated successfully.
Mar 21 22:20:20 UbuntuDVWAlab8 systemd[1]: Finished sysstat-collect.service - system activity accounting tool.
Mar 21 22:22:19 UbuntuDVWAlab8 systemd-timesyncd[445]: Network configuration changed, trying to establish connection.
Mar 21 22:25:01 UbuntuDVWAlab8 CRON[2284]: pam_unix(cron:session): session opened for user root(uid=0) by root(uid=0)
Mar 21 22:25:01 UbuntuDVWAlab8 CRON[2285]: (root) CMD (command -v debian-sa1 > /dev/null && debian-sa1 1 1)
Mar 21 22:25:01 UbuntuDVWAlab8 CRON[2284]: pam_unix(cron:session): session closed for user root
Mar 21 22:27:19 UbuntuDVWAlab8 systemd-timesyncd[445]: Network configuration changed, trying to establish connection.
Mar 21 22:30:21 UbuntuDVWAlab8 systemd[1]: Starting sysstat-collect.service - system activity accounting tool…
Mar 21 22:30:21 UbuntuDVWAlab8 systemd[1]: sysstat-collect.service: Deactivated successfully.
Mar 21 22:30:21 UbuntuDVWAlab8 systemd[1]: Finished sysstat-collect.service - system activity accounting tool.
Mar 21 22:30:27 UbuntuDVWAlab8 ubuntu[2294]: salut
2025-03-21T22:31:16-03:00 freebsd sshd[3637] Received disconnect from 192.168.2.8 port 37746:11: disconnected by user
2025-03-21T22:31:16-03:00 freebsd sshd[3637] Disconnected from user root 192.168.2.8 port 37746
2025-03-21T22:31:24-03:00 freebsd sshd[3707] Accepted keyboard-interactive/pam for root from 192.168.2.8 port 32922 ssh2
Mar 21 22:31:49 UbuntuDVWAlab8 sshd[2258]: Received disconnect from 192.168.2.8 port 51750:11: disconnected by user
Mar 21 22:31:49 UbuntuDVWAlab8 sshd[2258]: Disconnected from user ubuntu 192.168.2.8 port 51750
Mar 21 22:31:49 UbuntuDVWAlab8 sshd[2201]: pam_unix(sshd:session): session closed for user ubuntu
Mar 21 22:31:49 UbuntuDVWAlab8 systemd[1]: session-34.scope: Deactivated successfully.
Mar 21 22:31:49 UbuntuDVWAlab8 systemd[1]: session-34.scope: Consumed 1.094s CPU time.
Mar 21 22:31:49 UbuntuDVWAlab8 systemd-logind[644]: Session 34 logged out. Waiting for processes to exit.
Mar 21 22:31:49 UbuntuDVWAlab8 systemd-logind[644]: Removed session 34.
Mar 21 22:31:54 UbuntuDVWAlab8 sshd[2296]: Accepted password for ubuntu from 192.168.2.8 port 40512 ssh2
Mar 21 22:31:54 UbuntuDVWAlab8 sshd[2296]: pam_unix(sshd:session): session opened for user ubuntu(uid=1000) by ubuntu(uid=0)
Mar 21 22:31:54 UbuntuDVWAlab8 systemd-logind[644]: New session 38 of user ubuntu.
Mar 21 22:31:54 UbuntuDVWAlab8 systemd[1]: Started session-38.scope - Session 38 of User ubuntu.
Mar 21 22:32:20 UbuntuDVWAlab8 systemd-timesyncd[445]: Network configuration changed, trying to establish connection.
Mar 21 22:35:01 UbuntuDVWAlab8 CRON[2365]: pam_unix(cron:session): session opened for user root(uid=0) by root(uid=0)
Mar 21 22:35:01 UbuntuDVWAlab8 CRON[2366]: (root) CMD (command -v debian-sa1 > /dev/null && debian-sa1 1 1)
Mar 21 22:35:01 UbuntuDVWAlab8 CRON[2365]: pam_unix(cron:session): session closed for user root

Files :: Text Filters ::                                                                                   Press TAB to edit
```